

CIS HPE Aruba Networking CX Switch Benchmark

v1.0.1 - 01-08-2026

Terms of Use

Please see the below link for our current terms of use:

<https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/>

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is **NEVER** acceptable to host a CIS Benchmark in **ANY** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Terms of Use	1
Table of Contents	2
Overview	6
Important Usage Information	6
Key Stakeholders	6
Apply the Correct Version of a Benchmark	7
Exceptions	7
Remediation	8
Summary	8
Target Technology Details	9
Intended Audience.....	9
Consensus Guidance	10
Typographical Conventions.....	11
Recommendation Definitions.....	12
Title.....	12
Assessment Status.....	12
Automated	12
Manual.....	12
Profile	12
Description.....	12
Rationale Statement	12
Impact Statement.....	13
Audit Procedure.....	13
Remediation Procedure.....	13
Default Value.....	13
References	13
CIS Critical Security Controls® (CIS Controls®)	13
Additional Information.....	13
Profile Definitions	14
Acknowledgements	15
Recommendations	16
1 Management.....	16
1.1 Securing Switch Management Access	17
1.1.1 Create security user group (Manual)	18
1.1.2 Securing Password Entry (Manual)	20
1.1.3 Hardening Password Rules (Automated)	22

1.1.4 Set an Export Password (Automated)	24
1.1.5 Enable Enhanced Secure Mode (Manual).....	26
1.1.6 Default admin account password (Manual)	29
1.1.7 RBAC - Customer defined local user groups (Manual)	31
1.1.8 Session Management (Automated)	33
1.1.9 Verifying Telnet Server is Disabled (Automated).....	36
1.1.10 Using Local RBAC to Limit User Access to Shell (Manual).....	38
1.2 Securing SSH	41
1.2.1 SSH Public Key Authentication (Automated).....	42
1.2.2 SSH Allow List (Automated)	44
1.2.3 SSH Server Port Customization (Automated)	47
1.2.4 Recommended Ciphers, MACs, and Algorithms (Manual).....	49
1.2.5 Two-factor authentication with the SSH server (Automated)	53
1.2.6 SSH Server Key (Manual)	55
1.3 Securing Time Synchronization	59
1.3.1 NTP Authentication (Automated).....	60
1.3.2 Configuring Time Services (Automated).....	63
NTP Client:	65
NTP Conductor:.....	65
1.4 Securing SNMP Access	67
1.4.1 SNMP Community	68
1.4.1.1 Non Default Community Names, Access Rights & ACL (Automated).....	69
1.4.2 SNMPv3 Enablement	71
1.4.2.1 SNMP V3 (Automated)	72
1.4.3 SNMP Traps (Automated)	74
1.5 AAA for Management Interfaces	77
1.5.1 Remote AAA Servers	78
1.5.1.1 Radius Server Configuration (Automated).....	79
1.5.1.2 TACACS Server Configuration (Automated)	82
1.5.1.3 RadSec Server Configuration (Manual).....	85
1.5.2 Authentication	89
1.5.2.1 Default & Fallback Local Authentication (Manual).....	90
1.5.2.2 Limit Login Attempts (Automated)	92
1.5.2.3 Remote Authentication - RADIUS/RadSec/TACACS+ (Automated).....	95
1.5.3 Authorization	97
1.5.3.1 Local Authorization (Automated)	98
1.5.3.2 Remote Authorization (Automated)	100
1.5.4 Accounting.....	103
1.5.4.1 Local Accounting (Automated).....	104
1.5.4.2 Remote Accounting (Automated).....	106
1.5.5 Per User Management Interface Enablement (Manual).....	108
1.5.6 Login Privilege Elevation for Administrators (Automated)	111
1.6 Public Key Infrastructure (PKI).....	113
1.6.1 TLS Check Key Usage (Manual)	114
1.6.2 TLS Minimum Version (Automated).....	116
1.7 Firmware	119
1.7.1 Firmware Validation (Manual).....	120
1.8 Securing File Transfer	122
1.8.1 SCP and SFTP	123
1.8.1.1 SFTP and SCP (Manual).....	124
1.9 Securing the https-server	126
1.9.1 https-server default enablement (Automated)	127
1.9.2 https-server idle session management (Automated).....	129
1.9.3 Two-factor authentication with the https-server server (Automated).....	131
1.9.4 Assign a custom certificate to the https-server (Manual)	133
1.10 Enable ServiceOS Password Authentication.....	135

1.10.1 ServiceOS Password (Automated)	136
1.11 Securing Syslog	138
1.11.1 Assign a custom certificate to syslog-client (Manual)	139
1.11.2 Configure syslog-client to log using TLS (Automated)	141
1.12 Login Banner (Automated)	143
1.13 Schedule Configuration Backup Job (Automated)	145
1.14 Create Hostname (Automated)	149
2 Interface	151
2.1 Physical Security	152
2.1.1 Disable USB and Bluetooth on Device (Automated)	153
2.1.2 Front Panel Security (Manual)	155
2.1.3 Disable Unused Physical Interfaces (Manual)	157
2.2 Traffic Control - Rate limiting (Manual)	159
2.3 Proxy ARP (Manual)	162
2.4 IP Directed Broadcast (Manual)	164
3 Protocol	166
3.1 Routing Protocols	166
3.1.1 OSPF	167
3.1.1.1 OSPF Passive Interfaces (Manual)	168
3.1.1.2 OSPF Neighbor Authentication (Manual)	171
3.1.1.3 OSPFv3 Area Authentication and Encryption with IPsec (Manual)	173
3.1.2 BGP	176
3.1.2.1 Control Plane ACL for BGP Peering Sessions (Manual)	177
3.1.2.2 Authenticate BGP Peers Using MD5 (Manual)	179
3.1.2.3 BGP TTL Security (Manual)	181
3.2 DHCP Protocols	183
3.2.1 DHCP Snooping	184
3.2.1.1 DHCPv4 & DHCPv6 Snooping Enablement (Manual)	185
3.2.1.2 DHCPv6 Guard (Manual)	188
3.3 Multicast	191
3.3.1 PIM	192
3.3.1.1 PIM Accept-Register (Manual)	193
3.3.1.2 PIM Accept-RP (Manual)	195
3.3.1.3 PIM SSM (Manual)	197
3.3.2 SSDP (Manual)	199
3.3.3 IGMP Snooping ACL (Manual)	202
3.3.4 MLD Snooping ACL (Manual)	204
3.3.5 MSDP Authentication & SA Filtering (Manual)	206
3.3.6 MSDP SA Cache limit (Manual)	208
3.3.7 Multicast Boundary ACL (Manual)	210
3.3.8 Multicast BSR Boundary (Manual)	212
3.4 IP Source Lockdown (Manual)	214
3.5 Dynamic ARP Inspection (Manual)	216
3.6 ND Snooping (Manual)	218
3.7 RA Guard (Manual)	220
3.8 IPv6 Destination Guard (Manual)	223
4 Control Plane	225
4.1 COPP Policing	226
4.1.1 Control Plane Policing (Manual)	227
4.2 Spanning Tree Security	233
4.2.1 Spanning Tree BPDU Protect (Manual)	234
4.2.2 Spanning Tree Root Protect (Manual)	237
4.3 Control Plane ACL	239
4.3.1 Control Plane ACL Management (Manual)	240

<i>Appendix: Summary Table</i>	<i>242</i>
<i>Appendix: CIS Controls v7 IG 1 Mapped Recommendations</i>	<i>248</i>
<i>Appendix: CIS Controls v7 IG 2 Mapped Recommendations</i>	<i>250</i>
<i>Appendix: CIS Controls v7 IG 3 Mapped Recommendations</i>	<i>253</i>
<i>Appendix: CIS Controls v7 Unmapped Recommendations.....</i>	<i>256</i>
<i>Appendix: CIS Controls v8 IG 1 Mapped Recommendations</i>	<i>257</i>
<i>Appendix: CIS Controls v8 IG 2 Mapped Recommendations</i>	<i>259</i>
<i>Appendix: CIS Controls v8 IG 3 Mapped Recommendations</i>	<i>262</i>
<i>Appendix: CIS Controls v8 Unmapped Recommendations.....</i>	<i>265</i>
<i>Appendix: Change History</i>	<i>266</i>

Overview

All CIS Benchmarks™ (Benchmarks) focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the Benchmarks are designed to be a key **component** of a comprehensive cybersecurity program.

Important Usage Information

All Benchmarks are available free for non-commercial use from the [CIS Website](#). They can be used to manually assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- [CIS Configuration Assessment Tool \(CIS-CAT® Pro Assessor\)](#)
- [CIS Benchmarks™ Certified 3rd Party Tooling](#)

These tools make the hardening process much more scalable for large numbers of systems and applications.

NOTE: Some tooling focuses only on the Benchmark Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that **ALL** Recommendations (**Automated** and **Manual**) be addressed since all are important for properly securing systems and are typically in scope for audits.

Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To assure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.
- **Use the most recent version of a Benchmark:** This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.

Remediation

CIS has developed [Build Kits](#) for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's "Remediation" section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

When remediating systems (changing configuration settings on deployed systems as per the Benchmark's Recommendations), please approach this with caution and test thoroughly.

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
 - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
 - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
 - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
 - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
 - When the initial deployment above is completed successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

NOTE: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the [CIS Website](#). All other formats of the CIS Benchmarks™ (MS Word, Excel, and [Build Kits](#)) are available for CIS [SecureSuite](#)® members.

CIS-CAT® Pro is also available to CIS [SecureSuite](#)® members.

Target Technology Details

This document, Security Configuration Benchmark for HPE Aruba Networking CX Switch, provides prescriptive guidance for establishing a secure configuration posture for HPE Aruba Networking CX Switches running AOS-CX version 10.16.1006 or later. This guide was tested against AOS-CX version 10.16.1006. This is a development version and is meant to encourage the HPE Aruba user community to test configurations and make recommendations. Please note that certain features described in this document may not be available on all switch platforms. For a comprehensive list of supported features for each platform, kindly refer to the HPE Aruba Networking Support Portal - <https://networkingsupport.hpe.com/>

To obtain the latest version of this guide, please visit <http://benchmarks.cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at benchmarkinfo@cisecurity.org.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate HPE Aruba Networks AOS-CX on an HPE Aruba Networks switching platforms.

Consensus Guidance

This CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
<code>Monospace font</code>	Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.
<code><Monospace font in brackets></code>	Text set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
Bold font	Additional information or caveats things like Notes , Warnings , or Cautions (usually just the word itself and the rest of the text normal).

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) "4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

Items in this profile intend to:

- be practical and prudent;
- provide a clear security benefit; and
- not inhibit the utility of the technology beyond acceptable means.

- **Level 2**

This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount
- acts as a defense in depth measure
- may negatively inhibit the utility or performance of the technology.

- **Optional Security Recommendations**

This profile extends the "Level 2" profile. The optional security recommendations for AOS-CX switches provide advanced guidelines that extend beyond Level 2 benchmarks, catering to specific network configurations and use cases.

These recommendations focus on enhancing security in areas such as advanced routing, multicast, network defense and feature-specific configurations, which may not be universally applicable to all customers.

They are designed to offer tailored security enhancements for customers who deploy and utilize specific network features, ensuring a flexible and adaptable approach to securing diverse environments

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Special Thanks to the entire HPE Aruba Networks team for their dedication and assistance in creating this benchmark.

Author

Shobana Nandakumar

Contributor

Darren Stevenson

Phil White

Tabitha Haug

Editor

Shaun Wakumoto

Matt Claiborne

Jeff Jones

Recommendations

1 Management

Securing the management plane of Aruba CX switches is essential to protect network configurations and administrative functions from unauthorized access and cyber threats. This involves using features like role-based access control (RBAC), secure protocols (SSH, HTTPS), multi-factor authentication (MFA), and many more. By enforcing best practices and leveraging the advanced security capabilities of Aruba CX switches, organizations can protect their network management interfaces against potential threats, ensuring operational continuity and data integrity across their IT environments.

1.1 Securing Switch Management Access

1.1.1 Create security user group (Manual)

Profile Applicability:

- Level 1

Description:

This sequence creates a new local user group which can be used for security administrators.

Rationale:

Some organizations have a security officer which has a subset of responsibilities compared to an administrator. A security administrator should be able to view, clear, and copy the security logs on the device.

Impact:

The use of a built-in administrators or operators account for the security officer would provide an excess of access to the device.

Audit:

Create the security administrator group with the following:

```
switch(config)# user-group <group>
switch(config-usr-grp-<group>)# permit cli command "show security-logs*"
switch(config-usr-grp-<group>)# permit cli command "clear security-logs"
switch(config-usr-grp-<group>)# permit cli command "copy security-log*"
switch(config-usr-grp-<group>)# exit
```

Security administrators can be added to this new group through the following:

```
switch(config)# user <name> group <group> password
Adding user <name>
Enter password:*****
Confirm password:*****
```

Remediation:

Perform the following to determine if the security role is available:

```
switch# show user-group | include <group>
```

Default Value:

The security administrator group is not available by default.

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Chp_Mng_Use/use-def-use-gro-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 <u>Establish and Maintain an Inventory of Accounts</u> Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			
v7	4.1 <u>Maintain Inventory of Administrative Accounts</u> Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.			

1.1.2 Securing Password Entry (Manual)

Profile Applicability:

- Level 1

Description:

This section describes a method of obfuscating or masking password or shared secret entry.

Rationale:

Entering passwords or shared secrets can be a source of information leakage if someone can observe the data entry or if the terminal command history can be accessed. Password Masking or obfuscation prevents this leakage by not displaying these values in the console session.

Impact:

Not utilizing password masking exposes secure credential values to anyone with access to the terminal display during entry or to the console command history.

Audit:

Remediation:

The password masking function is accessed by

example - creating a new user:

```
switch(config)# user switchAdmin group administrators password
Enter password: *****
Confirm password: *****
switch(config)#
```

example - changing a user password:

```
switch(config)# user switchAdmin password
Enter password: *****
Confirm password: *****
switch(config)#
```

example - configuring a radius host shared secret:

```
switch(config)# radius-server host 10.10.10.10 key
Enter the RADIUS server key: *****
Re-Enter the RADIUS server key: *****
switch(config)#
```

Default Value:

Password Masking is an entry method and not a setting. There is no default value

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.			

1.1.3 Hardening Password Rules (Automated)

Profile Applicability:

- Level 1

Description:

It is critical that customers set good, strong passwords for their local user accounts. The password complexity feature can aid customers in ensuring that users are following company password policies.

Rationale:

There are many known attack vectors against weak passwords. The use of strong passwords guard against such attacks and is recommended across all of computing. Password complexity allows administrators to define a set of password rules which can then align with their company's password policy. The password complexity allows for minimum password length, minimum lowercase/uppercase/special/numeric characters, position changes between passwords, and can protect against password reuse. CIS Recommends 14 characters or more in length with 1 Uppercase, 1 Lowercase, 1 Number and 1 Special Character.

Impact:

Use of weak or easily guessed passwords can result in unintended access of the device and could lead to someone taking over the network.

Audit:

Review the password complexity configuration:

```
6200# show password-complexity
Global password complexity checking criteria:
  Password complexity                : Enable
  Previous passwords to check        : 5
  Minimum password length            : 14
  Minimum position changes           : 8
  Maximum adjacent characters count   : 0
  Password composition
    Minimum lowercase characters      : 1
    Minimum uppercase characters      : 1
    Minimum special characters        : 1
    Minimum numeric characters        : 1
```

Remediation:

Set a password complexity policy with a minimum of <X> characters long, includes at least <Y> lowercase/uppercase/special/numeric character, and doesn't allow users to reuse the past <Z> passwords:

```

switch(config)# password complexity
switch(config-pwd-cplx)# minimum-length <X>
switch(config-pwd-cplx)# lowercase-count <Y>
switch(config-pwd-cplx)# uppercase-count <Y>
switch(config-pwd-cplx)# special-char-count <Y>
switch(config-pwd-cplx)# numeric-count <Y>
switch(config-pwd-cplx)# history-count <Z>
switch(config-pwd-cplx)# enable

```

Sample recommended password complexity configuration based on
<https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>

```

switch(config)# password complexity
switch(config-pwd-cplx)# minimum-length 8
switch(config-pwd-cplx)# lowercase-count 1
switch(config-pwd-cplx)# uppercase-count 1
switch(config-pwd-cplx)# special-char-count 1
switch(config-pwd-cplx)# numeric-count 1
switch(config-pwd-cplx)# history-count 1
switch(config-pwd-cplx)# enable

```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Chp_Mng_Use/User_grp_cmds/pas-complx.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.7 Manage Default Accounts on Enterprise Assets and Software Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.2 Change Default Passwords Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

1.1.4 Set an Export Password (Automated)

Profile Applicability:

- Level 1

Description:

All AOS-CX switches ship with a default password that's used to export any customer secrets contained with the switch configuration. Display of secrets through 'show' commands or exporting the entire switch configuration will have its secrets encrypted with this password prior to being displayed. AOS-CX allows customers to set their own password to ensure that their switch secrets cannot be loaded onto another AOS-CX switch.

Rationale:

AOS-CX switch configurations and secrets can be loaded onto another AOS-CX switch. If a customer exports their configuration using the default export password, it can be loaded into another switch.

Impact:

Secrets are never exposed in plaintext, but loading of another switch's secrets onto another could enable that other device to impersonate another switch in the network. This may include, but not limited to, MACsec peering with an MKA PSK or OSPFv2 shared secrets.

Audit:

View the state of export password:

```
switch# show service export-password
Export password: default
```

After configuring custom export password:

```
switch# show service export-password
Export password: custom
```

Remediation:

Set a custom export password using the following command:

```
switch(config)# service export-password
Enter password: *****
Confirm password: *****
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Chp_Mng_Use/User_grp_cmds/ser-exp-pas.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			
v7	<u>4.2 Change Default Passwords</u> Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.			

1.1.5 Enable Enhanced Secure Mode (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

This sequence describes enabling enhanced secure mode

Rationale:

The AOS-CX operating system provides access to the underlying Linux system, allowing administrators to launch a bash shell session from the switch command-line interface. This shell provides root-level access to the underlying Linux OS.

Impact:

Misuse of shell access could expose sensitive network traffic to an unauthorized third party via packet mirroring to a remote device or could cause a denial of service by modifying or removing system files. This file modification could render the device unbootable, and require software restoration through the ServiceOS console..

The following are best practices for limiting shell access:

Disable access to the Bash shell by changing the switch security mode to enhanced from ServiceOS. Limit shell access by using RBAC or an external TACACS+ authorization server to deny access to the start-shell command to all users except those who specifically require it.

Audit:

```
switch# show secure-mode
Standard secure mode is set
switch#
```

Remediation:

```
switch(config)# boot system serviceos
One time boot to ServiceOS initiated.
Checking if the configuration needs to be saved...

This will reboot the system to ServiceOS and render
the entire switch unavailable.
Access to ServiceOS is only available through the serial console.
Continue (y/n)? y

Default boot image set to serviceos.
The system is going down for reboot.
...
ServiceOS login: admin
SVOS>
SVOS> secure-mode enhanced
#####WARNING#####
This will set the switch into enhanced secure mode. Before
enhanced secure mode is enabled, the switch must securely erase
all customer data and reset the switch to factory defaults.
This will initiate a reboot and render the switch unavailable
until the zeroization is complete.
#####WARNING#####

Continue (y/n)? y
reboot: Restarting system
...
6300 login: admin
Password:

Please configure the 'admin' user account password.
Enter new password: *****
Confirm new password: *****
switch#
switch# show secure-mode
Enhanced secure mode is set
switch#
```

Default Value:

Standard secure mode is set by default

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/hardening/Content/Chp_hard-mgmt/lim-shell-acc.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v7	<u>4.3 Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.			

1.1.6 Default admin account password (Manual)

Profile Applicability:

- Level 1

Description:

The AOS-CX switches ship with a built-in, default user account named 'admin'. In accordance with the 2020 California password law, AOS-CX switches require that customers set the password for this built-in user account at first login.

Rationale:

The setting of a strong password for all built-in user account is necessary for any device.

Impact:

AOS-CX devices will force customers to set a password for the built-in 'admin' user account upon first login. It's important that customers abide by this behavior to ensure that their device isn't deployed with a weak or empty password.

Audit:

There is no audit procedure as the first time a customer logs into the device, they will be required to provide a password for the built-in 'admin' user account.

Remediation:

If a customer fails to set a strong password for the built-in 'admin' user account, he/she can set the password using the following command:

```
switch(config)# user admin password
Enter password: *****
Confirm password: *****
switch(config)#
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Chp_Mng_Use/def-use-adm-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			
v7	<u>4.2 Change Default Passwords</u> Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.			

1.1.7 RBAC - Customer defined local user groups (Manual)

Profile Applicability:

- Level 1

Description:

AOS-CX switches include three different built-in local user groups: administrators, operators, auditors. Administrators have full read-write access, operators have read-only access, and auditors can read the logs. There may be scenarios where customers need a local user group with a different set of permissions. User-defined local user groups allow customers to create their own user group with specific CLI commands allowed for members of that group.

Rationale:

The built-in local user groups may not be sufficient to meet customer needs in how their assign permissions to different local user accounts.

Impact:

The built-in local user accounts have a very string read-write, read-only, and read-logs set of permissions. There may be instances where customers need to allow local users to write access to some switch features, but not all.

Audit:

The "show user group" command allows customers to see the set of local user groups configured on the switch:

switch(config)# show user-group			
GROUP NAME	GROUP TYPE	INCLUDED GROUP	NUMBER OF RULES
-----	-----	-----	-----
administrators	built-in	n/a	n/a
auditors	built-in	n/a	n/a
operators	built-in	n/a	n/a
routing-group	configuration	admuser1	10
switch(config)#			

Remediation:

Create local user groups as needed:

```
switch(config)# user-group group
switch(config-usr-grp-group)# 10 permit cli command "<command>"
switch(config-usr-grp-group)# 20 permit cli command "<command>"
switch(config-usr-grp-group)# exit
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Chp_Mng_Use/use-def-use-gro-10.htm
2. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Chp_Mng_Use/User_grp_cmds/use-gro-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.12 Segment Data Processing and Storage Based on Sensitivity Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.			
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			
v7	14.1 Segment the Network Based on Sensitivity Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).			
v7	16.6 Maintain an Inventory of Accounts Maintain an inventory of all accounts organized by authentication system.			

1.1.8 Session Management (Automated)

Profile Applicability:

- Level 1

Description:

This sequence describes enabling CLI session limits

Rationale:

Session management enhances security by enforcing specific CLI user session requirements for console, SSH and telnet connections.

The following information is provided at the time of a successful login:

- When applicable, the number of failed login attempts since the most recent successful login.
- The date, time, and location (console or IP address or hostname) of the most recent previous successful login.
- The count of successful logins within the past (configurable) time period.

The Recommendation of CIS is to use the following as a minimum setting

```
cli-session
  max-per-user 1
  tracking-range 25
  timeout 15
```

Impact:

Limiting concurrent sessions and session timeouts is crucial for enhancing security and preventing unauthorized access to accounts. Failure to restrict the number of active sessions per user and setting appropriate timeout durations, can expose you to risks like session hijacking, shared account access, and compromised sessions.

Audit:

To view the configuration change -

```
switch# show running-config | begin cli-session
cli-session
  max-per-user 1
  tracking-range 25
  timeout 15
```

Remediation:

Setting Max sessions per user:

```

switch# config
switch(config)# cli-session
switch(config-cli-session)# max-per-user <max-sessions>
switch(config-cli-session)# exit
switch(config)# exit
switch#

```

Setting session timeout:

```

switch# config
switch(config)# cli-session
switch(config-cli-session)# timeout <timeout in minutes>
switch(config-cli-session)# exit
switch(config)# exit
switch#

```

Setting session tracking records retention:

```

switch# config
switch(config)# cli-session
switch(config-cli-session)# tracking-range <tracking days>
switch(config-cli-session)# exit
switch(config)# exit
switch#

```

Recommended values -

```

switch(config)# cli-session
switch(config-cli-session)# max-per-user 1
switch(config-cli-session)# timeout 15
switch(config-cli-session)# tracking-range 25
switch(config-cli-session)# exit

```

Default Value:

The default values for session management parameters are: max sessions per user: 5 session timeout 30 (minutes) session tracking-range 30 (days)

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/hardening/Content/Chp_hard-mgmt/session.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			
v7	16.13 <u>Alert on Account Login Behavior Deviation</u> Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			

1.1.9 Verifying Telnet Server is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

AOS-CX system includes a telnet server. Telnet is considered insecure primarily because it transmits all data, including usernames and passwords, in plaintext, meaning it's not encrypted. This leaves it vulnerable to several security risks:

Eavesdropping: Anyone with access to the network traffic can intercept and read the data transmitted during a Telnet session, including sensitive information like login credentials.

Credential Sniffing: Attackers can easily capture plaintext usernames and passwords by observing Telnet traffic.

Man-in-the-Middle (MitM) Attacks: Attackers can position themselves between the client and server, intercepting, reading, and potentially modifying the data being transmitted, according to Kelvin Zero.

Session Hijacking: With intercepted credentials, attackers can hijack ongoing Telnet sessions, gaining unauthorized access to systems and data.

Lack of Authentication: Many Telnet implementations lack proper authentication mechanisms, making them vulnerable to attacks like brute-force attacks.

In summary, Telnet's fundamental design, which involves unencrypted data transmission, makes it highly insecure and unsuitable for modern remote access, especially over public networks like the internet. Instead of Telnet, it is recommended to use Secure Shell (SSH), which provides encryption for data transmission and strong authentication mechanisms, ensuring a much higher level of security for remote access.

Rationale:

Telnet server is included in AOS-CX system for customer convenience. Due to its insecurity it is not recommended for general use and is disabled by default.

Impact:

Verifying Telnet server is disabled will prevent users from accessing the console using an insecure protocol

Audit:

To display telnet server status:

```
switch(config)# show telnet server
TELNET server is not enabled on any VRFs.
switch(config)#
```

Remediation:

to disable Telnet server:

```
switch(config)# no telnet server vrf <vrf>
All active TELNET sessions on the VRF will be terminated.
Do you want to continue (y/n)? y
switch(config)#
```

Default Value:

Telnet server is disable by default.

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.10/HTML/cli_6200/Content/Chp_telnet/telnet_cmds/tel-serv.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

1.1.10 Using Local RBAC to Limit User Access to Shell (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

AOS-CX switches include three different built-in local user groups: administrators, operators, auditors. Administrators have full read-write access, operators have read-only access, and auditors can read the logs. There may be scenarios where customers need a local administrator user with a different set of permissions. User-defined local user groups allow customers to create their own user group with specific CLI commands allowed for members of that group, including access to the underlying OS shell.

Rationale:

The built-in local user groups may not be sufficient to meet customer needs in how they assign permissions to different local user administrator accounts. This can be utilized to allow customers to create users with access to administrator-level commands while limiting access to the underlying OS shell.

Impact:

The underlying Linux OS allows full access to all features of the AOS-CX system. Many administrative functions do not require access to this level of control. Limiting access to the shell helps limit exposure to both malicious and unintentional system changes.

Audit:

The "show user-group" command allows customers to see the set of local user groups configured on the switch:

```
switch(config)# show user-group
GROUP NAME      GROUP TYPE      INCLUDED GROUP  NUMBER OF RULES
-----
custom-admin    configuration    --              4
administrators  built-in        n/a             n/a
auditors        built-in        n/a             n/a
operators       built-in        n/a             n/a
routing-group   configuration    admuser1        10
switch(config)#
```

the show user-group command displays user group status and any Rules configured:

```
switch(config)# show user-group custom-admin
```

```
User Group Summary
```

```
=====
```

```
Name           : custom-admin
Type           : configuration
Included Group  : --
Number of Rules : 4
```

```
User Group Rules
```

```
=====
```

SEQUENCE NUM	ACTION	COMMAND	COMMENT
--------------	--------	---------	---------

-----	-----	-----	-----
-------	-------	-------	-------

10	deny	start-shell	
20	deny	user .*	
30	deny	user-group .*	
500	permit	.*	

```
switch(config)#
```

Remediation:

Create local user groups as needed:

```
switch(config)# user-group group
switch(config-usr-grp-group)# 10 permit cli command "<command>"
switch(config-usr-grp-group)# 20 permit cli command "<command>"
switch(config-usr-grp-group)# exit
switch(config)#
```

Create user group rules to restrict access to underlying shell, and ability to modify the user-group rules:

```
switch(config)# user-group custom-admin
switch(config-usr-grp-admin2)# 10 deny cli command "start-shell"
switch(config-usr-grp-admin2)# 20 deny cli command "user .*"
switch(config-usr-grp-admin2)# 30 deny cli command "user-group .*"
switch(config-usr-grp-admin2)# 500 permit cli command ".*"
switch(config-usr-grp-admin2)# exit
switch(config)#
```

Default Value:

default administrator users have no restriction on access to the underlying OS shell.

References:

1. <https://arubanetworking.hpe.com/techdocs/AOS-CX/10.07/PDF/5200-7885.pdf>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.13 <u>Deploy a Data Loss Prevention Solution</u> Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			●
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●
v7	14.7 <u>Enforce Access Control to Data through Automated Tools</u> Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.			●

1.2 Securing SSH

SSH server allows remote access the management plane of AOS-CX devices. Securing SSH server is critical to controlling access the management interface.

1.2.1 SSH Public Key Authentication (Automated)

Profile Applicability:

- Level 2

Description:

This sequence describes configuring public-key authentication

Rationale:

Passwords are easy to use and remember, but they are vulnerable to attacks and human errors. Keys are more secure and efficient compared to passwords. SSH Public key authentication is enabled by default and takes precedence over password-based authentication. Validate users identified with SSH public keys stored in the local user database using the following commands.

Impact:

Public-key authentication uses a cryptographic pair of keys, public and private, to verify user identity and secure communication. A user's private key is kept securely on the device used to connect to the switch. The user's public key is configured on the switch as an authorizing key for that user. SSH public-key authentication is enabled (by default) on the switch to allow user connectivity.

Audit:

```
switch# Show user <username> authorized-key <user public-key>

switch# show ssh authentication-method
SSH publickey authentication      : Enabled
SSH password authentication      : Enabled
SSH two factor authentication     : Disabled
SSH certificate as authorized-key : Disabled

switch#
```

Remediation:

```
switch(config)# user <username> authorized-key <user public-key>
Added SSH client's authorized-key with key-identifier 1.

switch(config)#
```

Default Value:

The user's ssh authentication key is not configured by default. The ssh server public-key authentication method is enabled by default.

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_832x-8400-9300-10000/Content/Chp_SSH_serv/ssh-ser.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.			
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.			

1.2.2 SSH Allow List (Automated)

Profile Applicability:

- Level 1

Description:

This sequence describes configuring SSH access control list

Rationale:

SSH server allow-list allows the switch admin to limit in-bound SSH connections to be from specific ip addresses or networks.

Note that system access control lists can also limit in-bound SSH traffic, depending on how they are configured. If an ACL is applied to the control-plane and the SSH allow-list is also enabled, the control-plane ACL has pre-emption over the SSH allow-list.

Impact:

Configure a list of addresses that will be the only hosts allowed to connect to the SSH servers running on all VRFs of the switch. By default, the allow-list is disabled and any host is allowed to connect given the correct authentication criteria. When the allow-list is enabled, only the hosts that fall under one of the entries may connect with the correct authentication criteria, all other hosts will be denied to attempt authentication.

Audit:

```
switch# show ssh server allow-list
SSH server allow-list:

Status: Enabled

Allowed host IPs:
  1.1.1.1
  2.2.2.0/24
  10::10
  20:20::/64

switch#
```

Remediation:

```
switch(config)# ssh server allow-list
switch(config-ssh-al)# ip 1.1.1.1
switch(config-ssh-al)# ip 2.2.2.0/24
switch(config-ssh-al)# ipv6 10::10
switch(config-ssh-al)# ipv6 20:20::/64
switch(config-ssh-al)# enable
Active SSH sessions will be terminated.
Do you want to continue (y/n)? y

switch(config-ssh-al)# exit
switch(config)#
```

Default Value:

The SSH server allow-list is not configured or enabled by default.

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_832x-8400-9300-10000/Content/Chp_SSH_serv/SSH_serv_cmds/ssh-ser-all-lis.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	3.13 Deploy a Data Loss Prevention Solution Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>14.6 Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			
v7	<u>14.7 Enforce Access Control to Data through Automated Tools</u> Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.			

1.2.3 SSH Server Port Customization (Automated)

Profile Applicability:

- Optional Security Recommendations

Description:

This sequence describes configuring which IP port SSH server listens on

Rationale:

By default, SSH server listens on TCP port 22. This port will be used for all VRFs that have SSH server enabled. Optionally AOS-CX switches provides the ability to modify the default SSH server port to add extra protection to the server.

Impact:

Configuring a SSH server listening port allows admins to provide ssh connectivity to the switch when network situations, such as business networks and wifi hotspots, block IP port 22.

Audit:

```
switch# show ssh server

SSH server configuration on VRF default :

    IP Version      : IPv4 and IPv6      SSH Version      : 2.0
    TCP Port        : 44444              Grace Timeout (sec) : 60
    Max Auth Attempts : 6                Server Status     : running
    SFTP Server      : disabled

    ...

switch(config)#
```

Remediation:

```
switch# conf
switch(config)# ssh server port 44444
Active SSH sessions will be terminated.
Do you want to continue (y/n)? y
switch(config)#
```

Default Value:

The SSH server allow-list is not configured or enabled by default.

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_832x-8400-9300-10000/Content/Chp_SSH_serv/SSH_serv_cmds/ssh-ser-prt.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			
v7	12.4 <u>Deny Communication over Unauthorized Ports</u> Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.			

1.2.4 Recommended Ciphers, MACs, and Algorithms (Manual)

Profile Applicability:

- Level 1

Description:

This sequence describes configuring SSH server ciphers, MACs, and algorithms

Rationale:

SSH server ciphers, MACs, and algorithms allow the admin to select specific values for SSH encryption, allowing for flexibility and/or greater security in the SSH sessions.

Impact:

SSH ciphers , message authentication codes (MACs), and algorithms are based on OpenSSH's default settings and are deemed secure by the community.

For highly secure deployments like Federal Accounts which mandates the compliance of NDcPP (Common Criteria Protection Profile), it is recommended to configure more secure ciphers , MACs, and algorithms as per the NDcPP evaluation criteria.

Audit:

```
switch# show ssh server

SSH server configuration on VRF default :

    IP Version      : IPv4 and IPv6      SSH Version       : 2.0
    TCP Port        : 22                  Grace Timeout (sec) : 60
    Max Auth Attempts : 6                  Server Status      : running
    SFTP Server      : disabled

Allow-list: disabled

Ciphers:
chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr,
aes128-gcm@openssh.com, aes256-gcm@openssh.com

Host Key Algorithms:
ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521,
ssh-ed25519, rsa-sha2-256, rsa-sha2-512, ssh-rsa

Key Exchange Algorithms:
curve25519-sha256, curve25519-sha256@libssh.org, ecdh-sha2-nistp256,
ecdh-sha2-nistp384, ecdh-sha2-nistp521

MACs:
hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com,
hmac-sha1-etm@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1

Public Key Algorithms:
rsa-sha2-256, rsa-sha2-512, ssh-rsa, ecdsa-sha2-nistp256,
ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-ed25519,
x509v3-rsa2048-sha256, x509v3-ssh-rsa, x509v3-sign-rsa,
x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384,
x509v3-ecdsa-sha2-nistp521

switch#
```

Remediation:

```
switch(config)# ssh ciphers aes128-ctr aes256-ctr aes128-cbc aes256-cbc
switch(config)# ssh macs hmac-sha2-256 hmac-sha2-512 hmac-sha1
switch(config)# ssh key-exchange-algorithms ecdh-sha2-nistp256 ecdh-sha2-
nistp384 diffie-hellman-group14-sha1
switch(config)# ssh host-key-algorithms ecdsa-sha2-nistp256 ecdsa-sha2-
nistp384 ecdsa-sha2-nistp521
switch(config)# ssh public-key-algorithms ecdsa-sha2-nistp256 ecdsa-sha2-
nistp384 ecdsa-sha2-nistp521
switch(config)#
```

Default Value:

Ciphers: [chacha20-poly1305@openssh.com](#), aes128-ctr, aes192-ctr, aes256-ctr, [aes128-gcm@openssh.com](#), [aes256-gcm@openssh.com](#)

Host Key Algorithms: ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-ed25519, rsa-sha2-256, rsa-sha2-512, ssh-rsa

Key Exchange Algorithms: curve25519-sha256, curve25519-sha256@libssh.org, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521

MACs: hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha1-etm@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1

Public Key Algorithms: rsa-sha2-256, rsa-sha2-512, ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-ed25519, x509v3-rsa2048-sha256, x509v3-ssh-rsa, x509v3-sign-rsa, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_832x-8400-9300-10000/Content/Chp_SSH_serv/SSH_serv_cmds/ssh-ser-com63.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 <u>Encrypt Data on End-User Devices</u> Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.			
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v8	16.11 <u>Leverage Vetted Modules or Services for Application Security Components</u> Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	13.6 <u>Encrypt the Hard Drive of All Mobile Devices.</u> Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.		●	●
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●
v7	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.		●	●
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●
v7	18.5 <u>Use Only Standardized and Extensively Reviewed Encryption Algorithms</u> Use only standardized and extensively reviewed encryption algorithms.		●	●

1.2.5 Two-factor authentication with the SSH server (Automated)

Profile Applicability:

- Optional Security Recommendations

Description:

Two-factor authentication provides an additional level of security by requiring administrators to perform X.509 certificate-based authentication with the AOS-CX SSH server. The two factors are possession of the certificate private key and knowledge of the password associated with the certificate private key.

The switch must be configured with the corresponding CA certificate which issued the administrator's certificate.

Rationale:

Customers with a large number of administrators can be configuration and maintenance challenge across a large network. Use of certificate-based and two-factor authentication can simplify this maintenance for customers.

Impact:

Any changes in administrator user passwords or the additional or removal of administrator accounts can become a maintenance headache for customers. Use of two-factor authentication only requires the enablement of the feature and the addition of the corresponding CA certificate as a trust anchor.

Audit:

Two factor authentication configuration can be checked using the "show ssh authentication-method" command:

```
switch(config)# show ssh authentication-method
SSH publickey authentication      : Enabled
SSH password authentication      : Enabled
SSH two factor authentication    : Disabled
SSH certificate as authorized-key : Disabled
```

Trust Anchor (TA) profiles can be viewed using the "show crypto pki ta-profile" command:

```
switch(config)# show crypto pki ta-profile
TA Profile Name          TA Certificate          Revocation Check
-----
root-ca-for-ssh-server   Installed, valid        disabled
switch(config)#
```

Remediation:

```
switch(config)# ssh certificate-as-authorized-key
switch(config)# ssh two-factor-authentication authorization local
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Chp_Rem_AAA_RADIUS/config-two-fac-aut.htm
2. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Chp_PKI/ins-cer-roo-ca-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 <u>Require MFA for Externally-Exposed Applications</u> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.			
v8	6.5 <u>Require MFA for Administrative Access</u> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.			
v7	4.5 <u>Use Multifactor Authentication For All Administrative Access</u> Use multi-factor authentication and encrypted channels for all administrative account access.			
v7	16.3 <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

1.2.6 SSH Server Key (Manual)

Profile Applicability:

- Level 1

Description:

This sequence describes configuring the SSH server keys.

Rationale:

An SSH server key, also known as a host key, is a cryptographic key that identifies an SSH server to a client. It's generated when the SSH server is enabled and acts as a digital fingerprint, ensuring the server's identity during the connection process.

Impact:

Weak SSH host keys create significant security risks by making systems vulnerable to attack. Attackers can exploit weak keys to intercept or manipulate communications, steal sensitive data, or even gain unauthorized access to the server. Among the risks associated with weak SSH-server keys are:

- Man in the middle (MITM) attacks
- Server identity spoofing
- Key theft and impersonation
- Unauthorized access
- Compromised user credentials
- Compliance issues

To mitigate these risks it is important to:

- Generate Strong Keys
- Use strong cryptographic algorithms and key lengths when generating SSH host keys
- Rotate Keys Regularly
- Use a Key Management System
- Monitor SSH Connections
- Disable Weak Algorithms

Audit:

To show all ssh server keys:

```

switch# show ssh host-key

Key Type : ECDSA      Curve : ecdsa-sha2-nistp256
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBP8HHn/kuFLkTcOr/3mcF39N3
iTJpJt1Ek1XgBzm55y58/+S1EDykV0e8O0AKQU8A2Oy28kFh44U6oV/F7nKa8U= user@switch

Key Type : ED25519
ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAILT4vG7j10sLWwgoPnoDPMMc7TGqYB7WrEi11E816UPF
user@switch

Key Type : RSA      Key Size : 3072
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGC3dZwFsNtuqmr5+Ls83YIRsgwgSa83udFlbY+Qipy8/Uoh
NijXDbSRU4no+bCSvJ1YpF9dWLT5HxrwTVRRYhzDwSRZwkFZLTHs5kflrR1dcQ193M16/dOBMNycI
dHOErV40B7KTs/61won8cVtOc/O9cWKFnlEAWyznmf3JgVUGwKB5zAn+heQ0u6vUGCEJiImdnqUqt
/f2Kaw+mHFNBoerzMNSx1QDBB3raIJxZPHB6RMtdUT2UdG/fV+XfaiYAqyyeMKWdFHdqCky2ykYec
IgoI5OtQGdRQM3QHWYpcChRTsWfJIu0uvfQsn3OXemZw1KcaWck/rDO8SAE5CxYBN6dET53pSktjf
q7WIK9CpVy21ISCqJmLrZbjLGJBGEevRilKVvBY+vOj3rcymqc+6z1GoMfqvObl4wds6jBjebweOS
ygw9SnmQ5EmIrbnsjnv0eOLh/F+jwCcAnmEe0lgEwcdQOi2QdBe6UeX8yyBitZk9N5zsxa5rnPGGo
cBbU= user@switch

switch#

```

To show the ECDSA server keys:

```

switch# show ssh host-key ecdsa

Key Type : ECDSA      Curve : ecdsa-sha2-nistp256
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBP8HHn/kuFLkTcOr/3mcF39N3
iTJpJt1Ek1XgBzm55y58/+S1EDykV0e8O0AKQU8A2Oy28kFh44U6oV/F7nKa8U= user@switch

switch#

```

To show the ED25519 server keys:

```

switch# show ssh host-key ed25519

Key Type : ED25519
ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAILT4vG7j10sLWwgoPnoDPMMc7TGqYB7WrEi11E816UPF
user@switch

switch#

```

To show the RSA server keys:

```
switch# show ssh host-key rsa
Key Type : RSA          Key Size : 3072
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGC3dZwFsNtuqmr5+Ls83YIRsgwgSa83udFlbY+Qipy8/Uoh
NijXDbSRU4no+bCSvJ1YpF9dWLT5HxrwTVRRYhzDwSRZwkFZLTHs5kflrR1dcQ193M16/dOBMNycI
dHOErV40B7KTs/61won8cVtOc/O9cWKFnleAWyznmf3JgVUGwKB5zAn+heQ0u6vUGCEJiImdnqUqt
/f2Kaw+mHFNBoeRzMNSx1QDBB3raIJxZPHB6RMtdUT2UdG/fV+XfaiYAqyyeMKWdFHdqCky2ykYec
IgoI5OtQGdRQM3QHWYpcChRTsWfJIu0uvfQsn3OXemZw1KcaWck/rD08SAE5CxYBN6dET53pSktjf
q7WIK9CpVy21ISCqJmLrZbjLGJBGEevRi1KVvBY+vOj3rcymqc+6z1GoMfqvOb14wds6jBjebweOS
ygy9SnmQ5EmIrbnsjnv0eOLh/F+jwCcAnmEe0lgEwcdQOi2QdBe6UeX8yyBitZk9N5zsxa5rnPGGo
cBbU= user@switch

switch#
```

Remediation:

To set ssh server key:

```
switch(config)# ssh host-key <key-type> <curve/bits>
```

To set a nistp256 ecdsa server-key:

```
switch(config)# ssh host-key ecdsa ecdsa-sha2-nistp256
ecdsa host-key will be overwritten.
Do you want to continue (y/n)? y
switch(config)#
```

to set an ed25519 server-key:

```
switch(config)# ssh host-key ed25519
ed25519 host-key will be overwritten.
Do you want to continue (y/n)? y
switch(config)#
```

To set a 256-bit RSA server-key:

```
switch(config)# ssh host-key rsa bits 2048
rsa host-key will be overwritten.
Do you want to continue (y/n)? y
switch(config)#
```

Default Value:

SSH server is enabled on the Default and Mgmt (if applicable) VRFs by default. When the SSH server is enabled for the first time, the following SSH server keys are generate:

- ecdsa-sha2-nistp256
- ed25519
- 2048-bit RSA keys.

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/AOSCX-CLI-Bank/cli_8360/Content/Chp_SSH_serv/SSH_serv_cmds/ssh-hos-key55.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v8	16.11 <u>Leverage Vetted Modules or Services for Application Security Components</u> Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.			
v7	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.			
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.			
v7	18.5 <u>Use Only Standardized and Extensively Reviewed Encryption Algorithms</u> Use only standardized and extensively reviewed encryption algorithms.			

1.3 Securing Time Synchronization

Many secure protocols and auditing functions rely on system times being synchronized with a reliable time source, either within or (where security considerations permit) external to the managed network. One of the most commonly-used protocols to accomplish this is the Network Time Protocol (NTP), which can use both local and Internet-hosted servers to synchronize system time across a network. Recommendation - NTP should be configured and enabled on the device prior to enabling secure management protocols.

A common practice among organizations that span multiple time zones is to use NTP to synchronize time clocks and set the local time zone on all equipment to UTC. This practice aids in troubleshooting and security audits for devices that might be continents apart. Both IPv4 and IPv6 Servers are supported.

1.3.1 NTP Authentication (Automated)

Profile Applicability:

- Level 1

Description:

This sequence describes configuring NTP authentication.

Rationale:

Many secure protocols and auditing functions rely on system times being synchronized with a reliable time source, either within or (where security considerations permit) external to the managed network. Network Time Protocol (NTP) is used to synchronize clocks on networked devices, ensuring consistent timestamps for various applications. This is crucial for tasks like accurate logging, security analysis, and reliable operation of distributed systems.

Impact:

NTP authentication support allows the NTP client to verify that servers are in fact known and trusted and not intruders intending accidentally or intentionally to masquerade as a legitimate server.

Audit:

```
switch# show ntp servers
-----
NTP SERVER      KEYID    MINPOLL  MAXPOLL  OPTION  VER
-----
10.100.1.254    --       6        10      none    4 prefer
10.80.2.219     --       6        10      iburst  4 prefer(auto)
pool.ntp.org    --       4         4      iburst  4
-----

switch# show ntp authentication-keys
-----
-----
Key ID    Trusted  Type      Encrypted Key
-----
-----
1         No       MD5       AQBapUtt1YTjZS2PH4+J7G5OKJG0GuZ2WxmD0339TNg6nfGXY=
-----
--

switch# show ntp status
NTP Status Information
NTP                      : Enabled
NTP DHCP                 : Enabled
NTP Authentication       : Enabled
NTP Server Connections   : Using the mgmt VRF
System time              : Fri Mar  8 03:51:46 PST 2024
NTP uptime               : 8 days, 15 hours, 24 minutes, 37 seconds
Not synchronized with an NTP server.
```

Remediation:

```
switch(config)# ntp authentication
switch(config)# ntp authentication-key 1 md5 <ntpauthkey>
switch(config)# ntp server 10.10.10.10 prefer
switch(config)# ntp vrf mgmt
```

Default Value:

NTP authentication is not configured or enabled by default

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/hardening/Content/Chp_hard-mgmt/time-sync.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v8	16.11 <u>Leverage Vetted Modules or Services for Application Security Components</u> Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.			
v7	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.			
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.			
v7	18.5 <u>Use Only Standardized and Extensively Reviewed Encryption Algorithms</u> Use only standardized and extensively reviewed encryption algorithms.			

1.3.2 Configuring Time Services (Automated)

Profile Applicability:

- Level 1

Description:

This sequence describes configuring time services. AOS-CX supports both NTP client and NTP server functionality. NTP client can be configured manually or via DHCP option 42.

Rationale:

Network Time services are used to synchronize computer clocks across a network, ensuring accurate and consistent timekeeping for various applications and services. This synchronization is crucial for tasks like file system updates, network management, security, and distributed systems. Network Time Protocol (NTP) provides a reliable source of accurate time that can enable time synchronization between multiple devices dispersed across any network.

Impact:

Inaccurate timekeeping between network devices can lead to many undesirable results including:

- inability to correlate events between devices, making debugging difficult.
- failure of network authentication services, as many require time synchronization to operate.
- time-based network attacks that exploit the time settings differences in network devices.
- operational and security best practice is to configure more than 1 NTP server

Audit:

to view the NTP configuration:

```
switch0(config)# show run | include ntp
ntp server 10.10.10.10 minpoll 10 maxpoll 14 iburst prefer
ntp server 20.20.20.20
ntp enable
ntp vrf mgmt
ntp conductor vrf default stratum 4
switch(config)#
```

To view NTP status:

```
switch# show ntp status
NTP Status Information
```

```
NTP : Enabled
NTP DHCP : Enabled
NTP Authentication : Disabled
NTP Server Connections : Using the mgmt VRF

System time : Mon Jun 30 15:40:40 PDT 2025
NTP uptime : 10 days, 3 hours, 52 minutes, 19 seconds
```

NTP Synchronization Information

```
NTP Server : 10.10.10.10 at stratum 4
Poll interval : 1024 seconds
Time accuracy : Within 0.000836 seconds
Reference time : Mon, Jun 30 2025 15:05:34.146 as per
America/Los_Angeles
```

To view NTP associations:

```
switch# show ntp associations
```

ID	NAME	REMOTE	REF-ID	ST	LAST	POLL	REACH
+ 1	10.10.10.10	10.10.10.10	10.10.100.100	3	702	1024	377
+ 2	20.20.20.20	20.20.20.20	20.20.200.200	4	776	1024	377

```
switch#
```

To show NTP server info:

```
switch# show ntp servers
```

NTP SERVER	KEYID	MINPOLL	MAXPOLL	OPTION	VER
10.10.10.10	--	6	10	iburst	4 prefer
20.20.20.20	--	6	10	iburst	4

```
switch#
```

To show NTP associations:

```
switch# show ntp associations
```

ID	NAME	REMOTE	REF-ID	ST	LAST	POLL	REACH
+ 1	10.10.10.10	10.10.10.10	10.10.100.100	3	702	1024	377
+ 2	20.20.20.20	20.20.20.20	20.20.200.200	4	776	1024	377

```
switch
```

Remediation:

Note: In order for the NTP process to associate with a server, the switch time must be set to within 15 minutes of the NTP server time.

To set switch time:

```
switch(config)# clock datetime YYYY-MM-DD HH:MM:SS
switch(config)# clock timezone <timezone>
switch(config)#
```

NTP Client:

Configure an NTP time source:

```
switch(config)# ntp server <DNS-name or IP-address> <optional parameters>
switch(config)#
```

Note: Optional parameters:

burst	NTP Association use burst mode
iburst	NTP Association use iburst mode
key-id <4-17>	NTP Key ID
maxpoll <4-17>	NTP maximum poll time to use configuration
minpoll <4-17>	NTP minimum poll time to use configuration
prefer	NTP Association preference configuration
version <3-4>	NTP Association version configuration

To allow NTP server being set via DHCP option 42:

```
switch(config)# ntp dhcp-enable
switch(config)#
```

To specify a VRF for NTP to listen on:

```
switch(config)# ntp vrf <vrf_name>
```

To enable NTP:

```
switch(config)# ntp enable
```

Example config of NTP client:

```
switch(config)# clock datetime 2025-06-30 14:22:00
switch(config)# clock timezone americas/los_angeles
switch(config)# ntp server 10.10.10.10 iburst minpoll 10 maxpoll 14 prefer
switch(config)# ntp server 20.20.20.20
switch(config)# ntp vrf mgmt
switch(config)# ntp enable
```

NTP Conductor:

Note:

- NTP clients and conductor must be enabled together. Configure NTP client first.
- NTP conductor MUST be enabled on a vrf other than the vrf of NTP client.

Configure an NTP Conductor:

```
switch(config)# ntp conductor stratum <1-15> vrf <vrf_name>
switch(config)#
```

Example config of and NTP conductor:

```
switch(config)# clock datetime 2025-06-30 14:22:00
switch(config)# clock timezone americas/los_angeles
switch(config)# ntp server 10.10.10.10 iburst minpoll 10 maxpoll 14 prefer
switch(config)# ntp vrf mgmt
switch(config)# ntp conductor stratum 4 vrf default
switch(config)# ntp enable
```

Default Value:

NTP is enabled on Mgmt VRF by default.

NTP server config via DHCP option 42 is enabled by default.

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.14/HTML/fundamentals_6300-6400/Content/Chp_IniCfg/NTP_cmds/ntp-com.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.			
v7	6.1 Utilize Three Synchronized Time Sources Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.			

1.4 Securing SNMP Access

Simple Network Management Protocol (SNMP) is an Internet-standard protocol used for managing and monitoring the devices connected to a network by collecting, organizing, and modifying information about managed devices on IP networks. There are three versions of the SNMP protocol: v1, v2c, and v3. SNMP is disabled by default on all AOS-CX devices. When enabled, SNMP provides limited write support in addition to read-only access and trap support for SNMP v1, v2c and v3. By securing SNMP, it reduce the risk of unauthorized access, protect sensitive data and maintain the reliability and integrity of the network infrastructure

1.4.1 SNMP Community

SNMPv1 and v2c use community names for read and write access. Much like passwords are used for authentication, these community names are sent across the wire as clear text. If a malicious user were to capture these community names, they could potentially issue SNMP set commands to make unauthorized and potentially harmful configuration changes to a network device.

1.4.1.1 Non Default Community Names, Access Rights & ACL (Automated)

Profile Applicability:

- Level 1

Description:

The default SNMP community name is public, a common setting for SNMP-capable devices.

Rationale:

Replace the public community name with another value that is hard to guess , but note that this doesn't fully prevent against attacks as this name is in clear text format in packet captures.

Impact:

By using a non-default (and strong) SNMP community name, you make it significantly harder for attackers to gain access to the SNMP interface of your devices.

Audit:

To view the snmp community configuration -

```
switch# show snmp community
```

Remediation:

The default access level for SNMP communities is read-only; if read-write support is required, set the access level for the community to rw from the community context. IPv4 and/or IPv6 ACLs may be used to limit access to allowed management stations or subnets; only one ACL (IPv4 or IPv6) may be applied to a community at a time. Apply an IPv4 or IPv6 ACL from the SNMP config-community context -

```
switch(config)# snmp-server community <community-name>
switch(config-community)# access-level <ro | rw>
switch(config-community)# access-list <IPv4 and/or IPv6 ACL>
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.13 <u>Deploy a Data Loss Prevention Solution</u> Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			●
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●
v7	14.7 <u>Enforce Access Control to Data through Automated Tools</u> Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.			●

1.4.2 SNMPv3 Enablement

SNMPv1 and v2c use community names for read and write access. Much like passwords are used for authentication, these community names are sent across the wire as clear text. If a malicious user were to capture these community names, they could potentially issue SNMP set commands to make unauthorized and potentially harmful configuration changes to a network device. SNMPv3, by comparison, utilizes a user-based security model with both authentication and privacy protocols to prevent unauthorized access or eavesdropping of management traffic. Best practices is to use SNMPv3 instead of older versions of SNMP.

1.4.2.1 SNMP V3 (Automated)

Profile Applicability:

- Level 2

Description:

SNMPv3, offers support for different users, authentication, and strong encryption. AOS-CX supports stronger authentication protocols (SHA224, SHA256, SHA384, and SHA 512) and privacy protocols (AES192 and AES256).

Rationale:

Enabling SNMPv3 enhances the security and reliability of network management by introducing authentication, encryption and message integrity features, addressing vulnerabilities present in earlier versions like SNMPv1 and SNMPv2c.

Impact:

Implementing SNMPv3 helps organizations meet security requirements and stay compliant with industry standards.

Audit:

To view the snmpv3 configuration and users -

```
switch# show run | in snmpv3
switch# show snmpv3 users
```

Remediation:

To create an SNMPv3 user using SHA for authentication and DES for privacy

```
switch(config)# snmpv3 user <myUser> auth sha auth-pass plaintext
<myAuthPswrd> priv
des priv-pass plaintext <myPrivPswrd>
```

Disable support for SNMPv1 and SNMPv2c and only accept SNMPv3 messages using the following command -

```
switch(config)# snmp-server snmpv3-only
```

To enable SNMP on the required VRF -

```
switch(config)# snmp-server vrf <vrf-name>
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>16.11 Leverage Vetted Modules or Services for Application Security Components</u> Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.			
v7	<u>18.5 Use Only Standardized and Extensively Reviewed Encryption Algorithms</u> Use only standardized and extensively reviewed encryption algorithms.			

1.4.3 SNMP Traps (Automated)

Profile Applicability:

- Level 2

Description:

Configuring SNMP (Simple Network Management Protocol) traps in AOS-CX switches enables proactive monitoring and management capabilities within the network infrastructure. SNMP traps act as automated notifications that are sent from the switches to a designated management system whenever specific events or thresholds occur, such as high cpu utilization, port status changes, or aaa server unreachability. This ensures real-time visibility into the health and performance of the switches. AOS-CX switches support multiple SNMP traps, which are either enabled by default or through configuration.

Rationale:

The rationale for configuring SNMP traps in AOS-CX switches lies in optimizing network operations and minimizing downtime. By enabling SNMP traps, administrators can quickly identify issues or changes in the switch environment without the need for constant manual monitoring. This configuration enhances efficiency, improves troubleshooting response times, and supports the overall stability and reliability of the network.

Impact:

Configuring SNMP traps in AOS-CX switches enables proactive issue detection, reducing downtime and improving response times.

Audit:

To view the list of snmp traps enabled -

```
switch# show run | in trap
```

Remediation:

Configure SNMPv2c trap

This command is used to configure the trap receivers to which the SNMP agent can send trap notifications -

```
snmp-server host <A.B.C.D | X:X::X:X> trap version <v1 | v2c> [community WORD] [port <UDP port>] [vrf <VRF_NAME>]
```

Configure SNMPv3 trap

This command is used to configure the trap receivers to which the SNMP agent can send SNMPv3 trap notifications.

```
snmp-server host <A.B.C.D | X:X::X:X> <trap | inform> version v3 user <WORD>
[port <UDP port>] [vrf <VRF_NAME>]
```

To enable specific snmp trap -

```
switch(config)# snmp-server trap
aaa-server-reachability-status Enable SNMP trap for AAA server
reachability
status
configuration-changes Enable configuration changes traps
cpu-utilization Enable high CPU utilization traps
link-status Enable link status traps for all physical
interfaces
mac-notify Enable MAC table change notification traps
memory-utilization Enable high memory utilization traps
module Enable module event traps
port-security Enable port-security violation traps.
(Default: enable)
rmon-events Enable RMON event traps
snmp Enable snmp traps
```

Default Value:

List of snmp traps enabled by default -

```
6300# show run all | in "snmp-server trap" snmp-server trap rmon-events snmp-server
trap cpu-utilization snmp-server trap memory-utilization snmp-server trap port-security
no snmp-server trap configuration-changes no snmp-server trap aaa-server-
reachability-status no snmp-server trap mac-notify snmp-server trap module snmp-
server trap link-status ifmib snmp-server trap link-status rmon
```

References:

1. https://www.arubanetworks.com/techdocs/AOS-CX/10.15/PDF/snmp_mib.pdf

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	8.11 Conduct Audit Log Reviews Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.			
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	6.7 Regularly Review Logs On a regular basis, review logs to identify anomalies or abnormal events.		●	●

1.5 AAA for Management Interfaces

AOS-CX have following management interfaces for accessing the switch for configuration and management -

- Console
- SSH
- Telnet
- https-server – Web UI and REST API

Telnet is not a recommended method to access the switch for configuration and management , as it is not a secure communication. It is not enabled by default on any VRF.

User accounts for accessing these management interfaces can be stored locally or managed on remote TACACS+ or RADIUS servers. AAA (Authentication, Authorization, and Accounting) is the security framework to manage user access, enforce privileges, and log the user access records.

1.5.1 Remote AAA Servers

AOS-CX Switches support following Remote AAA Servers -

1. RADIUS
2. RadSec
3. TACACS+

Using a remote AAA servers to manage logins reduces the need to save actual usernames and passwords on the device. It results in centralized secure management architecture. In case of Remote AAA unreachability, local AAA is considered as default fallback.

The following table describes supported AAA services based on the user account management methods:

1. Authentication -
 1. Local - Yes
 2. TACACS+ - Yes
 3. RADIUS / RadSec - Yes
2. Authorization -
 1. Local - Yes, RBAC
 2. TACACS+ - Yes, Per Command Authorization & RBAC
 3. RADIUS / RadSec - No
3. Accounting -
 1. Local - Yes
 2. TACACS+ - Yes
 3. RADIUS / RadSec - Yes

Supported Role assignment attributes using Remote AAA Servers -

1. RADIUS/RadSec
 - Aruba-Admin-Role VSA - Map the user to the matching local user-group name.
 - Aruba-Priv-Admin-User VSA - Extract the privilege level (1,15 & 19) and map the user to the local user-group corresponding to this privilege level (1=operators,15=administrators, 19=auditors). Privilege levels 2 to 14 may also be used with matching local user groups named 2 to 14.
 - RADIUS Service-Type - Map Administrative-User(6)to administrators and map NAS-Prompt-User(7) to operators.
2. TACACS+
 - Aruba-Admin-Role VSA - Map the user to the matching local user-group name.
 - TACACS+ priv-lvl attribute - Extract the privilege level (1,15 & 19) and map the user to the local user-group corresponding to this privilege level (1=operators,15=administrators, 19=auditors). Privilege levels 2 to 14 may also be used with matching local user groups named 2 to 14.

1.5.1.1 Radius Server Configuration (Automated)

Profile Applicability:

- Level 2

Description:

Remote AAA with RADIUS provides the following for your Aruba CX switch:

- Authentication using remote RADIUS AAA servers.
- Command authorization is not supported by RADIUS servers, however, user-defined local user

groups can be configured with command-authorization rules, providing locally configured per command authorization for members of such groups. See User-defined user groups . In the switch default state (without user-defined local groups), basic role-based authorization is available with the three built-in roles (administrators, operators, auditors).

- Transmission of locally collected accounting information to remote RADIUS servers.

Rationale:

Using a RADIUS server for AAA centralizes user management, ensuring uniform access policies across the network. It provides enhanced scalability, making it suitable for large networks with numerous users, compared to local AAA which is limited to individual switch.

Impact:

Implementing RADIUS SERVER for AAA, enhances security by minimizing the attack surface and ensuring compliance with industry standards for authentication.

Audit:

To view the radius-server configuration -

```
switch# show radius-server detail
```

Sample output -

```

switch# show radius-server detail
***** Global RADIUS Configuration *****

Shared-Secret           : None
Timeout                 : 5 seconds
Auth-Type               : pap
Retries                 : 1
DNS Query Mode          : Backoff
DNS Refresh Interval    : 300 seconds
Initial TLS Connection Timeout : 30 seconds
TLS Timeout             : 5 seconds
Tracking Time Interval  : 300 seconds
Tracking Retries        : 1
Tracking User-name      : radius-tracking-user
Tracking Password       : None
Status-Server Time Interval : 300 seconds
Number of Servers       : 2
AAA Server Status Trap  : Disabled

***** RADIUS Server Information *****
Server-Name             : 10.80.2.202
Auth-Port               : 1812
Accounting-Port         : 1813
VRF                     : mgmt
TLS Enabled             : No
Shared-Secret           :
AQBapedFhD6rT4Rh+Y8zhVPtwqDtliodV6pmWjR4Lq6riruQCAAAIDyC2NzNtyu
Timeout                 : 5 seconds
Retries                 : 1
Auth-Type               : pap
Msg-Authenticator-Check : disabled
Server-Group:Priority    : radius:1
ClearPass-Username      :
ClearPass-Password      : None
Tracking                : disabled
Tracking-Mode           : any
Reachability-Status     : unknown
Tracking-Last-Attempted : N/A
Next-Tracking-Request   : N/A

```

To view the aaa group configuration -

```
switch# show aaa server-groups radius
```

Sample output -

```
switch# show aaa server-groups radius

***** AAA Mechanism RADIUS *****
-----
GROUP NAME   | SERVER NAME       | TLS | PORT | VRF | PRIORITY
radius1      | radius1.lab.net   |     | 1812 | mgmt | 1
```

Remediation:

To Configure RADIUS Server -

```
switch(config)# radius-server host {<FQDN> | <IPv4> | <IPv6>} [key [plaintext
<PASSKEY> | ciphertext <PASSKEY>]] [vrf <VRF-NAME>]
```

To Associate RADIUS Server to the group -

```
switch(config)# aaa group server radius <group-name>
switch(config-sg) # server <FQDN | IPv4 | IPv6> vrf <vrf>
switch(config-sg) # exit
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Rem_AAA_cmds/rad-ser-hos-10.htm
2. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Rem_AAA_cmds/aaa-gro-ser.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 <u>Centralize Account Management</u> Centralize account management through a directory or identity service.			
v7	16.2 <u>Configure Centralized Point of Authentication</u> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.			

1.5.1.2 TACACS Server Configuration (Automated)

Profile Applicability:

- Level 2

Description:

TACACS+ is a centralized authentication, authorization, and accounting protocol that provides granular control over user access and command-level authorization for AOS-CX switches. It separates authentication, authorization, and accounting processes for enhanced flexibility.

Rationale:

TACACS+ supports per-command authorization, making it ideal for switches where granular control is needed. Unlike RADIUS, it encrypts entire packets, ensuring better security, and it offers more detailed logging for compliance purposes. Local authentication lacks scalability and centralized management, making TACACS+ preferable for larger networks.

Impact:

Implementing TACACS+ ensures improved security and centralized control, reducing the risk of unauthorized access or misconfiguration. It simplifies user management and audit trails, enhancing operational efficiency and compliance.

Audit:

To view the tacacs-server configuration -

```
switch# show tacacs-server detail
```

Sample output -

```

switch# show tacacs-server detail

***** Global TACACS+ Configuration *****

Shared-Secret:
AQBapb+HsdpqVlQ3CPCBMQTG8ekK1cA+CyD0RvfbeA8BEgikCgAAAJOWZSNzA2SWrLA=
Timeout: 5 seconds
Auth-Type: pap
Tracking Time Interval: 300 seconds
Tracking User-name: tacacs-tracking-user
Tracking Password: None
Number of Servers: 1

***** TACACS+ Server Information *****
Server-Name           : 1.1.1.1
Auth-Port             : 49
VRF                   : mgmt
Shared-Secret         :
AQBapfiTREWB7yUKCdmOMxMD26T0fQoXfJbtj9j2AUxlGn6eCAAAAF2MkfMTtojqX
Timeout              : 5 seconds
Auth-Type             : pap
Server-Group          : tacacs
Default-Priority       : 1
Tracking               : disabled
Reachability-Status   : N/A

```

To view the aaa group configuration -

```
switch# show aaa server-groups tacacs
```

Sample output -

```

switch# show aaa server-groups tacacs
***** AAA Mechanism TACACS+ *****
-----
GROUP NAME | SERVER NAME | PORT | VRF | PRIORITY
-----
tacacs    | 20.1.1.10  | 49   | default | 1

```

Remediation:

To Configure TACACS+ Server -

```
switch(config)# tacacs-server host {<FQDN> | <IPV4> | <IPV6>} [key [plaintext
<PASSKEY> | ciphertext <PASSKEY>]] [vrf <VRF-NAME>]
```

To Associate TACACS+ Server to the group -

```
switch(config)# aaa group server tacacs <group-name>
switch(config-sg) # server <FQDN | IPv4 | IPv6> vrf <vrf>
switch(config-sg) # exit
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Rem_AAA_cmds/aaa-gro-ser.htm
2. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Rem_AAA_cmds/tac-ser-hos-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.			
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.			

1.5.1.3 RadSec Server Configuration (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

RadSec Server: RadSec (RADIUS over TLS) is a secure extension of RADIUS that encrypts RADIUS communication using TLS. It provides secure authentication, authorization (through RBAC) and accounting for AOS-CX switches over untrusted networks like the WANs.

Rationale:

Unlike traditional RADIUS, which uses UDP and leaves communication vulnerable, RadSec ensures transport-layer encryption with TLS, offering enhanced security. RadSec is more suitable for environments where RADIUS traffic traverses public or untrusted networks. Local authentication, while simple, lacks centralized management and scalability.

Impact:

Deploying RadSec improves data security by ensuring all authentication traffic is encrypted, reducing the risk of interception or tampering. It is especially beneficial in distributed networks with remote sites. However, it may require additional certificate configurations, increasing operational complexity.

Audit:

To view the radius-server configuration -

```
switch# show radius-server detail
```

Sample output -

```

switch# show radius-server detail
***** Global RADIUS Configuration *****

Shared-Secret           : None
Timeout                 : 5 seconds
Auth-Type               : pap
Retries                 : 1
DNS Query Mode          : Backoff
DNS Refresh Interval    : 300 seconds
Initial TLS Connection Timeout : 30 seconds
TLS Timeout             : 5 seconds
Tracking Time Interval  : 300 seconds
Tracking Retries        : 1
Tracking User-name      : radius-tracking-user
Tracking Password       : None
Status-Server Time Interval : 300 seconds
Number of Servers       : 2
AAA Server Status Trap  : Disabled

***** RADIUS Server Information *****

Server-Name             : radius1.lab.net
Auth-Port               : 2083
Accounting-Port         : 2083
VRF                     : default
TLS Enabled             : Yes
TLS Connection Status   : tls_connection_established
Initial TLS Connection Timeout : 30 seconds
Timeout                 : 5 seconds
Auth-Type               : pap
Server-Group:Priority    : radius:2
ClearPass-Username      : 
ClearPass-Password      : None
Tracking                : disabled
Tracking-Mode           : any
Tracking-Method         : access-request
Reachability-Status     : unknown
Tracking-Last-Attempted : N/A
Next-Tracking-Request   : N/A
Port-Access Session     : status-server

```

To view the aaa group configuration -

```
switch# show aaa server-groups radius
```

Sample output -

```
switch# show aaa server-groups radius

***** AAA Mechanism RADIUS *****
-----
GROUP NAME   | SERVER NAME       | TLS | PORT | VRF | PRIORITY
radius1      | radius1.lab.net   | Yes | 2083 | mgmt | 1
```

Remediation:

Prerequisite for TLS - The RadSec connection between the switch and RadSec server requires TLS with mutual authentication. The switch and RadSec servers exchange digital certificates as a part of TLS mutual authentication. Also, RadSec mandates validating server certificates SAN/CN while establishing connections.

To associate the Leaf Certificate for RadSec -

```
switch(config)# crypto pki application radsec-client certificate
<certificate-name>
```

To Configure RadSec Server -

```
switch(config)# radius-server host {<FQDN> | <IPv4> | <IPv6>} tls [vrf <VRF-NAME>]
```

To Associate RadSec Server to the group -

```
switch(config)# aaa group server radius <group-name>
switch(config-sg) # server <FQDN | IPv4 | IPv6> tls vrf <vrf>
switch(config-sg) # exit
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Rem_AAA_cmds/aaa-gro-ser.htm
2. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Chp_Rem_AAA_RADIUS/sec-rad-rad-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.2 <u>Configure Centralized Point of Authentication</u> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.			
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.			

1.5.2 Authentication

Authentication identifies users, validates their credentials, and grants switch access. Authentication can be performed either locally or through Remote AAA Server - TACACS+ , RADIUS and RadSec. Most of the time, this is done through traditional username and password credential , but it could be extended to SSH Public Key & Two-Factor authentication. The following list describes supported authentication types based on their user account management methods -

Local -

1. Username and Password
2. SSH Public Key
3. SSH Two-Factor Authentication

TACACS+ -

1. Username and Password

RADIUS/RadSec -

1. Username and Password
2. SSH Two-Factor Authentication

1.5.2.1 Default & Fallback Local Authentication (Manual)

Profile Applicability:

- Level 2

Description:

Local user names and passwords are configured on a per-switch basis and provide the most basic form of authentication. Enabled by default for all management access connection types - console, SSH, and https-server (REST). Local authentication is also often used as the fallback login method. Local authentication can provide a minimum-security level should the primary method fail, but does not completely disable management access to the switch

Rationale:

Local authentication is a method where user credentials are stored directly on the AOS-CX switch itself, rather than relying on external authentication servers such as RADIUS/RadSec or TACACS+. This approach is particularly advantageous for infrastructures where remote authentication servers are either unavailable, unreliable, or impractical to deploy. This is especially important in small-scale networks, isolated environments, or edge deployments where remote servers may not be supported. Even in environments that support remote authentication servers, local authentication can serve as a fallback mechanism in case of server outages, network issues, or misconfigurations that prevent access to the remote server.

Impact:

Using local authentication in AOS-CX switches ensures reliable access in environments without remote server support, enhancing operational continuity. It simplifies deployment and reduces costs by eliminating the need for external authentication infrastructure. However, it lacks scalability, centralized control, and advanced logging, which could limit its effectiveness in larger or more complex networks. Organizations must ensure strong password policies and physical security to mitigate potential vulnerabilities.

Audit:

Local Authentication - Enabled by default for all connection types: console, SSH, and https-server (REST). Default – Includes all the management interfaces.

To view the configuration -

```
switch# show aaa authentication
```

Sample output -

```

switch# show aaa authentication
AAA Authentication:
  Fail-through           : Enabled
  Limit Login Attempts   : Not set
  Lockout Time           : 300
  Console Login Attempts : Not set
  Console Lockout Time   : 300

Authentication for default channel:
-----
GROUP NAME                | GROUP PRIORITY
-----
local                      | 0
-----

```

Remediation:

To configure a local administrator-level user named localadmin with interactive password entry:

```

switch(config)# user localadmin group administrators password
Enter password: *****
Confirm password: *****

```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Chp_Loc_AAA/Loc_AAA_cmds/sho-aaa-aut-dup-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			
v7	16.6 Maintain an Inventory of Accounts Maintain an inventory of all accounts organized by authentication system.			

1.5.2.2 Limit Login Attempts (Automated)

Profile Applicability:

- Level 2

Description:

The "Limiting Login Attempts" feature on Aruba AOS-CX switches is designed to enhance the security of the system by restricting the number of consecutive failed login attempts allowed for user accounts. Once the maximum number of failed attempts is reached, the account is blocked for a predetermined period - lockout-time. This local login attempt limiting feature is only available when not using remote authentication through AAA servers (TACACS+ or RADIUS) on any interface. Remote authentication through AAA servers (TACACS+ or RADIUS) is not possible when limit login attempts is configured on any interface.

Rationale:

Limiting login attempts on AOS-CX switches helps prevent brute-force attacks and unauthorized access, protecting critical network resources.

Impact:

This enhances security by safeguarding administrative accounts, reduces operational risks, and ensures compliance with security best practices.

Audit:

To view the configuration -

```
switch# show aaa authentication
```

Sample output -

```

switch# show aaa authentication
AAA Authentication:
  Fail-through           : Enabled
  Limit Login Attempts   : 3
  Lockout Time           : 60
  Console Login Attempts : 3
  Console Lockout Time   : 60

Authentication for default channel:
-----
GROUP NAME                | GROUP PRIORITY
-----
local                      | 0
-----

```

Remediation:

For the console interface (channel) only, enables console login attempt limiting. If the number of failed console login attempts equals the configured threshold, the user is locked out for the configured duration -

```

switch(config)# aaa authentication console-login-attempts <ATTEMPTS> console-
lockout-time <LOCKOUT-TIME>

```

For SSH/Telnet/https-server -

```

switch(config)# aaa authentication limit-login-attempts <ATTEMPTS> lockout-
time <LOCKOUT-TIME>

```

Sample recommendation -

Enabling login attempt failure limiting with a 60 second lockout being triggered upon the third consecutive login attempt failure -

```

switch(config)# aaa authentication console-login-attempts 3 console-lockout-
time 60
switch(config)# aaa authentication limit-login-attempts 3 lockout-time 60

```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Chp_Loc_AAA/Loc_AAA_cmds/aaa-auth_cons-log-att.htm
2. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Chp_Loc_AAA/Loc_AAA_cmds/aaa-aut-lim-log-att-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	16.13 <u>Alert on Account Login Behavior Deviation</u> Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

1.5.2.3 Remote Authentication - RADIUS/RadSec/TACACS+ (Automated)

Profile Applicability:

- Level 2

Description:

Remote Authentication involves the use of remote RADIUS , RadSec and TACACS+ servers for authenticating the management users. Remote AAA servers are used as single point of management to configure and store user accounts. They are often coupled with directories and management repositories, simplifying the setup and maintenance of the end-user accounts.

Rationale:

Remote authentication eliminates the need to manage local user accounts on each AOS-CX switch, simplifying administrative tasks and reducing the likelihood of configuration errors. Centralized control provided by remote servers allows for uniform enforcement of security policies, ensuring that all switches adhere to the same authentication and access standards.

Impact:

Remote authentication servers, such as RADIUS or TACACS+, allow seamless management of a large number of switches across distributed networks, enabling administrators to scale authentication across multiple devices without local configuration overhead.

Audit:

To view the configuration change -

```
switch# show aaa authentication
```

Sample output with two groups assigned for SSH -

```
switch# show aaa authentication
AAA Authentication:
  Fail-through           : Enabled
  Limit Login Attempts   : Not set
  Lockout Time           : 300
  Minimum Password Length : Not set
```

Authentication for ssh channel:

```
-----
GROUP NAME                | GROUP PRIORITY
-----
sg1                        | 0
sg2                        | 1
-----
```

Remediation:

Enable remote authentication for desired management interface. Default – Includes all the management interfaces -

```
switch(config)# aaa authentication login <console/default/ssh/telnet/https-
server> <RADIUS/TACACS+ group-list>
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Rem_AAA_cmds/sho-aaa-aut-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.5 Manage Access Control for Remote Assets Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v7	12.12 Manage All Devices Remotely Logging into Internal Network Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.			

1.5.3 Authorization

Authorization controls how authenticated users execute commands and interact with the switch. Authorization uses role-based access control (RBAC) to provide role-based privilege levels plus optional user-defined local user groups with command execution rules.

- TACACS+ Authorization - Upon successful user authentication, the user is assigned their role by the

TACACS+ server. See also User role assignment using TACACS+ attributes .TACACS+ authorization provides command filtering to allow/disallow individual command or command set execution. Each command is sent to the TACACS+ server for approval, and the switch then allows/disallows command execution according to the server response. TACACS+ authorization applies only to the CLI interface.

- RADIUS Authorization - Command authorization is not supported by RADIUS servers, however, user defined

local user groups can be configured with command-authorization rules, providing locally configured per command authorization for members of such groups.

- Fallback - Local authorization can be used as a fallback for the situation in which communication is

lost with all remote servers after a successful authentication. When defining the server access sequence for authorization, it is recommended to always include local as the last item in the list.

1.5.3.1 Local Authorization (Automated)

Profile Applicability:

- Level 1

Description:

Authorization controls authenticated users command execution and switch interaction privileges. Local authorization uses role-based access control (RBAC) to provide role-based privilege levels plus optional user-defined local user groups with command execution rules. Authorization occurs only after successful authentication.

- Administrators have full command execution and switch interaction privilege.
- Operators are limited to the use of several nonsensitive show commands.
- Auditors are limited to a few auditing-related commands.

Optional per-command authorization is available through configuration of user-defined local user groups with command authorization rules applied to respective group members.

Rationale:

Using local authorization on CX switches ensures faster authorization processes and eliminates dependency on external servers, enhancing reliability in scenarios where network connectivity to remote servers may be unavailable.

Audit:

To view the configuration change -

```
switch# show aaa authorization
```

Sample authorization output -

```
switch# show aaa authorization

***** Command authorization *****

Fail-through                      : Disabled

Authorization for default channel:
-----
GROUP NAME                        | GROUP PRIORITY
-----
local                             | 0
-----
```

Remediation:

To enable local as primary authorization method -

```
switch(config)# aaa authorization commands {default | console | ssh | telnet} local
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Chp_Loc_AAA/Loc_AAA_cmds/aaa-aut-com-dup-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.			
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.			

1.5.3.2 Remote Authorization (Automated)

Profile Applicability:

- Level 2

Description:

Remote authorization on CX switches leverages centralized servers like TACACS+ to manage and authorize user access, ensuring consistent enforcement of policies across the network.

Rationale:

Centralized remote authorization simplifies access management, enhances scalability, and provides a unified approach to monitoring and auditing user activities, reducing administrative overhead.

Impact:

This method strengthens security by centralizing control, ensures compliance with organizational policies, and allows for dynamic updates to access permissions, improving overall network governance and flexibility.

Audit:

To view the authorization configurations -

```
switch# show aaa authorization
```

Sample authorization output -

```
switch# show aaa authorization
```

```
***** Command authorization *****
```

```
Fail-through : Enabled
```

```
Authorization for console channel:
```

GROUP NAME	GROUP PRIORITY
sg1	0
local	1

```
Authorization for default channel:
```

GROUP NAME	GROUP PRIORITY
sg1	0
tacacs	1
local	2

```
Authorization for ssh channel:
```

GROUP NAME	GROUP PRIORITY
sg2	0

```
Authorization for telnet channel:
```

GROUP NAME	GROUP PRIORITY
sg2	0

Remediation:

To enable remote authorization by assigning the TACACS+ group list as primary method and local as recommended fallback method -

```
aaa authorization commands {default | console | ssh | telnet} group <tacacs-  
server-group-list> local
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Rem_AAA_cmds/aaa-aut-com-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 <u>Centralize Account Management</u> Centralize account management through a directory or identity service.			
v7	16.2 <u>Configure Centralized Point of Authentication</u> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.			

1.5.4 Accounting

Accounting in CX switches refers to tracking and logging user activities and access events for auditing and security purposes. It helps administrators monitor network behavior, troubleshoot issues, and ensure compliance with organizational policies. By integrating with external servers (e.g., RADIUS/TACACS+), CX switches provide detailed reports on user actions for enhanced visibility and governance.

1.5.4.1 Local Accounting (Automated)

Profile Applicability:

- Level 1

Description:

Local Accounting records all the CLI and REST access activities by users from all channels. It logs and helps to track all the configuration changes and show command executions happened at the switch for auditing or accounting purposes. This accounting information is captured and made available locally (Enabled by default and always active) and, if desired, for sending to remote AAA servers:

- Exec Accounting: user login/logout events.
- Command accounting: commands executed by users.
- System accounting: remote accounting On/Off events.
- Interactions on the non-CLI interfaces: REST and WebUI.

The following is not captured or made available as accounting information:

- CLI commands that reboot the switch.
- Interactions in the bash shell. (On the other hand, logging of “start-shell” CLI is supported . It helps in auditing)

Rationale:

Local accounting logs provide immediate access to user activity and configuration changes directly on the switch, ensuring visibility even when external logging systems are unavailable.

Impact:

Enhances operational resilience and supports faster troubleshooting during network outages or remote accounting server failures.

Audit:

To view accounting configuration -

```
switch# show aaa accounting
```

To view accounting logs -

```
switch# show accounting log
```

Sample outputs -

```

Bldg1-Acc-6300-VSF(config)# show aaa accounting
AAA Accounting:
  Accounting Type           : all
  Accounting Mode           : start-stop
  Accounting Fail-through   : Disabled

Accounting for default channel:
-----
GROUP NAME                  | GROUP PRIORITY
-----
local                       | 0
-----

Switch# show aaa accounting log all
-----
Command logs from previous boots
-----
2025-05-09T05:50:27.765+00:00 acctsyslogd[2788]: AUDIT|CLI "enable" executed
by user 'admin' from address '0.0.0.0' through CONSOLE session which resulted
in success at timezone UTC.

```

Remediation:

```
switch(config)# aaa accounting commands {exec|command|system} local
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Rem_AAA_cmds/sho-acc-log-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

1.5.4.2 Remote Accounting (Automated)

Profile Applicability:

- Level 2

Description:

For remote accounting, the information is sent to the first reachable remote server that was configured with this command for remote accounting. If no remote server is reachable, local accounting remains available by default

Rationale:

Implementing remote accounting enhances operational efficiency by providing real-time insights into network performance and security. It reduces the need for on-site management, streamlines troubleshooting, and ensures compliance with regulatory requirements through detailed reporting.

Impact:

Remote accounting improves network scalability and security, minimizes downtime through proactive monitoring, and reduces operational costs by enabling remote management of CX switches

Audit:

To view the configuration -

```
switch# show aaa accounting
```

Sample output -

```
(config)# show aaa accounting
AAA Accounting:
  Accounting Type           : all
  Accounting Mode           : start-stop
  Accounting Fail-through   : Enabled

Accounting for default channel:
-----
GROUP NAME                  | GROUP PRIORITY
-----
sg1                          | 0
```

Remediation:

To enable the remote accounting configuration:

```
Switch(config)# aaa accounting all-mgmt <console|default|https-  
server|ssh|telnet> start-stop <group>
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Rem_AAA_cmds/aaa-acc-all-mgm-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

1.5.5 Per User Management Interface Enablement (Manual)

Profile Applicability:

- Level 2

Description:

By default, authenticated users are enabled for accessing the switch through all these available management interfaces: ssh, telnet, https-server, console. Additionally fine-grained command authorization can be performed using RBAC , but it is applicable only for the CLIs not for Web-UI/REST API requests . Hence it is recommended to enable the specific management interfaces for the users based on the user type using below ways -

1. Local Per-User Management interface Enablement using CLI
2. Remote AAA Servers (Radius/ RadSec/ TACACS+) using VSA

Rationale:

Enabling a per-user management interface on Aruba AOS-CX switches allows network administrators to assign granular permissions and access rights to individual users. This tailored approach enhances the security posture of the network by restricting administrative privileges to only what is necessary for each user.

Impact:

Implementing per-user management ensures compliance with organizational access control policies, reducing the risk of unauthorized changes to the switch configuration.

Audit:

To view the configuration change -

```
switch(config)# show user-list management-interface
```

Sample Output -

```
switch(config)# show user-list management-interface
USER ENABLED MANAGEMENT INTERFACE(S)
-----
admin ssh,telnet,https-sever,console
admin1 telnet,https-server,console
```

Remediation:

Local per-user management interface enablement is performed with CLI command .
Example of disabling the SSH management interface for local user admin1 -

```
switch(config)# no user admin1 management-interface ssh
```

For remote TACACS+ and RADIUS/RadSec servers, per-user management interface enablement is performed by configuring the AOS-CX VSA Aruba-User-Mgmt-Interface (ID = 69 , type = string). On the TACACS+ or RADIUS/RadSec server, the AOS-CX VSA Aruba-User-Mgmt-Interface must be set to a comma-separated list of management interface names for which login is permitted by the associated user. Management interfaces omitted from the list are disabled for the associated user. A maximum of four management interface names are allowed, with each management interface name given once. Permitted management interface names (always lowercase) are as follows:

1. ssh
2. telnet
3. https-server
4. console

The VSA has a maximum length of 32 characters. The VSA is ignored by the switch if longer than 32 characters. When a user login fails because of an attempt to use a management interface that is not allowed, an event log is available indicating the enabled management interfaces as received in the TACACS+ or RADIUS/RadSec VSA.

Example Remote server VSA value that enables the two named management interfaces (ssh, telnet) while disabling the two unnamed management interfaces (https-server, console):

```
Aruba-User-Mgmt-Interface = "ssh,telnet"
```

Example Remote server VSA value that enables all four management interfaces:

```
Aruba-User-Mgmt-Interface = "ssh,telnet,https-server,console"
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Chp_Mng_Use/per-user-mgmt-intfc-cfg.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>12.8 Establish and Maintain Dedicated Computing Resources for All Administrative Work</u> Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.			●
v7	<u>4.3 Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●
v7	<u>4.6 Use of Dedicated Machines For All Administrative Tasks</u> Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.			●

1.5.6 Login Privilege Elevation for Administrators (Automated)

Profile Applicability:

- Level 2

Description:

By default, the AOS-CX switches only allow the administrator user to perform the "enable" command and when executed, the user is elevated in privilege without prompting for a password. To increase the security, login privilege elevation feature can be enabled. Configuration provided to enable/disable the privilege-elevation feature & will be disabled by default. The customer will have to enable this feature & then re-login for the privilege-elevation feature to take effect.. Upon successful login into the switch, the administrator user will be first provided with lower privilege access (the operator level access '>' prompt) and upon executing the 'enable' command, will be prompted to enter a password. The user will have to enter the same password and will be re-authenticated to elevate the privilege to administrator (the administrator level access with '#' prompt). Executing a disable will bring back the access to the '>' prompt

- Supported for Local/Radius/TACACS+ login authentications .
- Applicable to only users in administrator group and same password for both levels.

Rationale:

Every time a user runs the "enable" CLI, highly secure environments advise demanding a password.

Impact:

The impact of this feature enhances security and operational efficiency by ensuring that only trusted users gain administrative access after executing "enable" CLI.

Audit:

To view the configuration change -

```
switch# show run | in aaa
aaa authentication login privilege-elevation group administrators
```

Remediation:

To enable login privilege-elevation for group administrators -

```
Switch(config)# aaa authentication login privilege-elevation group administrators
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Chp_Loc_AAA/Loc_AAA_cmds/aaa-aut-priv-ele.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.			

1.6 Public Key Infrastructure (PKI)

The Public Key Infrastructure (PKI) feature enables administrators to manage digital certificates on the switch. The switch uses certificates to validate clients when acting as a server, and when communicating with servers when TLS encryption is used.

The AOS-CX Switch Series supports the installation of certificate authority (CA) certificates and the generation and installation of leaf certificates. The switch supports 64 trust anchor (TA) profiles. Each TA AOS-CX 10.13.1000 Hardening Guide | (All Switch Series) 36 profile stores a trusted CA certificate. The certificate can be either a root CA certificate, which must be self-signed, or an intermediate CA certificate that is issued by another CA. The TA profile also enables configuration of real-time checking of certificate revocation (through OCSP). Leaf certificates can be installed on the switch for use by applications such as:

- RadSec Client
- dot1x-suppliant
- EST Client
- captive-portal
- syslog client
- https-server - Web UI or REST API

AOS-CX switches by default supports the following preinstalled leaf certificates:

- **local-cert:** A self-signed certificate that switch automatically generated at first boot, as the default certificate for any application when the application's associated certificate is not configured
- **device-identity:** A device-identity certificate built into a switch at manufacturing and resident for the life of the product. The identity is a combination of an RSA key pair with physical information such as

the unit's model, chassis/PCA serial number, and base MAC ID.

Device Identity will be used for the following purposes:

- Allow 801.2X-2010 to perform peer authentication without the need for certificate or pre-shared key installation to automate the formation of MACsec secure channels between neighbor devices.
- Authentication with HPE Aruba Networking cloud services.

Certificate Name	Cert Status	EST Status
Associated Applications		
-----	-----	-----
local-cert	installed	n/a
est-client, hsc, https-server, radsec-client, syslog-client		
device-identity	installed	n/a
none		

1.6.1 TLS Check Key Usage (Manual)

Profile Applicability:

- Level 2

Description:

This sequence describes configuring TLS to enforce key usage checking

Rationale:

The Extended Key Usage X.509 v3 extension defines one or more purposes for which the public key can be used. This is in addition to or in place of the basic purposes specified by the Key Usage extension. As per NDcPP recommendation , that a peer certificate being used to establish TLS connection must have its extended key usage field set as client-auth or server-auth, depending on its role of the peer device. This configuration enables the checking of key usage during TLS handshake. It is disabled by default.

Audit:

```
switch# show tls
TLS crypto algorithms state: default
TLS key usage checking      : off
```

Remediation:

```
switch# conf
switch(config)# tls check-key-usage
```

Default Value:

off

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.		●	●
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

1.6.2 TLS Minimum Version (Automated)

Profile Applicability:

- Level 2

Description:

The switch supports TLS version 1.2 and 1.3 and secure cipher suites for each TLS version supported.

Rationale:

Audit:

Verify enabled TLS version and cipher suites:

```
switch# show tls global
```

```
Minimum TLS version : 1.2
```

```
TLS 1.2 cipher suites from highest to lowest priority :
```

State	Cipher Suite
-----	-----
allowed	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
allowed	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
allowed	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
allowed	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
allowed	TLS_RSA_WITH_AES_256_GCM_SHA384
allowed	TLS_RSA_WITH_AES_128_GCM_SHA256

```
TLS 1.3 cipher suites from highest to lowest priority :
```

State	Cipher Suite
-----	-----
allowed	TLS_AES_256_GCM_SHA384
allowed	TLS_AES_128_GCM_SHA256
allowed	TLS_CHACHA20_POLY1305_SHA256
allowed	TLS_AES_128_CCM_8_SHA256
allowed	TLS_AES_128_CCM_SHA256

```
TLS key exchange algorithms from highest to lowest priority :
```

State	Algorithm
-----	-----
allowed	secp521r1
allowed	secp384r1
allowed	secp256r1
allowed	X25519
allowed	X448
allowed	ffdhe8192
allowed	ffdhe6144
allowed	ffdhe4096
allowed	ffdhe3072
allowed	ffdhe2048

Remediation:

Default Value:

Default values:

```
switch# show tls global
```

Minimum TLS version : 1.2

TLS 1.2 cipher suites from highest to lowest priority :

State	Cipher Suite
-----	-----
allowed	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
allowed	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
allowed	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
allowed	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
allowed	TLS_RSA_WITH_AES_256_GCM_SHA384
allowed	TLS_RSA_WITH_AES_128_GCM_SHA256

TLS 1.3 cipher suites from highest to lowest priority :

State	Cipher Suite
-----	-----
allowed	TLS_AES_256_GCM_SHA384
allowed	TLS_AES_128_GCM_SHA256
allowed	TLS_CHACHA20_POLY1305_SHA256
allowed	TLS_AES_128_CCM_8_SHA256
allowed	TLS_AES_128_CCM_SHA256

TLS key exchange algorithms from highest to lowest priority :

State	Algorithm
-----	-----
allowed	secp521r1
allowed	secp384r1
allowed	secp256r1
allowed	X25519
allowed	X448
allowed	ffdhe8192
allowed	ffdhe6144
allowed	ffdhe4096
allowed	ffdhe3072
allowed	ffdhe2048

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.		●	●

1.7 Firmware

1.7.1 Firmware Validation (Manual)

Profile Applicability:

- Level 1

Description:

All AOS-CX switch firmware is signed by HPE at the time the firmware is created. The firmware signature is verified at the time of download and verified at every boot. The public keys used to verify the firmware is stored within the bootloader and firmware. The firmware is digitally signed with RSA-3072 and SHA-256. If the switch firmware validation fails at boot, the switch will fail to boot with one of the following error messages and drop the user into the ServiceOS login screen:

```
Error: Signature verification failed
Error: Signature not found
Error: Invalid signature
```

Rationale:

Firmware is validated when downloaded to the device and on every boot. A manual check can be done on the firmware images at any time.

Impact:

Firmware that fails validation will not be downloaded to the device. Firmware already on the device that fails validation will fail to boot.

Audit:

administrators can verify the firmware integrity using below show command before booting the switch. The verify option performs an integrity check that the image has a valid signature and is compatible with this system. The switch prevents the download of firmware without a valid signature.

```
switch# show images verify primary
The primary image is valid
switch# show images verify secondary
The secondary image is valid
```

Remediation:

Firmware without a valid signature will not boot. A new firmware image with a valid signature should be copied onto the device.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 <u>Address Unauthorized Software</u> Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v8	7.3 <u>Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v8	7.4 <u>Perform Automated Application Patch Management</u> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v8	12.1 <u>Ensure Network Infrastructure is Up-to-Date</u> Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.			
v7	2.6 <u>Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			
v7	3.4 <u>Deploy Automated Operating System Patch Management Tools</u> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.			
v7	3.5 <u>Deploy Automated Software Patch Management Tools</u> Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.			
v7	11.4 <u>Install the Latest Stable Version of Any Security-related Updates on All Network Devices</u> Install the latest stable version of any security-related updates on all network devices.			

1.8 Securing File Transfer

Secure File transfer protocols are essential for protecting sensitive data during file transfers. This is accomplished by encrypting data in transit, preventing unauthorized access and ensuring confidentiality.

The copy command is widely used in AOS-CX switches to transfer files, configurations and log messages. The commonly used file transfer protocol TFTP transfers files in plaintext, so attackers can easily capture transferred packets. To protect the device against security threats, it is recommended to use SFTP and SCP to perform the copy operations.

1.8.1 SCP and SFTP

This sequence describes using SCP and SFTP for secure file transfer

1.8.1.1 SFTP and SCP (Manual)

Profile Applicability:

- Level 1

Description:

The copy command is widely used in AOS-CX switches to transfer files, configurations and log messages. The commonly used file transfer protocol TFTP transfers files in plaintext, so attackers can easily capture and view the contents of transferred packets. Secure copy protocols encrypt the copy payload to prevent unwanted access to the transferred data

Rationale:

To protect malicious users from accessing the contents of transferred files, it is recommended to use SFTP and SCP to perform the copy operations.

Impact:

Transferring files using other methods, such as TFTP exposes the file contents in plaintext to anyone who has access to the data stream between the switch and the target. This can lead to disclosure of sensitive information to unwanted actors.

Audit:

The copy commands contains options for using SCP and SFTP as transfer protocols. examine the copy command to verify the source or destination is specified using the scp or sftp command

Remediation:

Select secure copy protocols when copying files to or from the switch. To copy a file to the device:

```
switch# copy scp://root@10.0.1.1/config running-config
```

or

```
switch# copy sftp://root@10.0.1.1/config running-config
```

To copy a file from the device:

```
switch# copy running-config scp://root@10.0.1.1/config cli
```

or

```
switch# copy running-config sftp://root@10.0.1.1/config cli vrf mgmt
```

Default Value:

there is no default value, the copy command options are user-specified.

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/hardening/Content/Chp_hard-mgmt/secure-copy.htm
2. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.11/HTML/cli_8400/Content/Chp_SpptCopy/SpptCopy_cmds/sup-cop-com.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

1.9 Securing the https-server

The https-server is used by both the REST API and WebUI.

1.9.1 https-server default enablement (Automated)

Profile Applicability:

- Level 1

Description:

On AOS-CX, the https-server is enabled by default allowing customers to access the device via its REST API or Web interface (WebUI). On campus products, the https-server is enabled on the default VRF. Products with an OOBM interface also have the https-server enabled on the mgmt VRF.

Rationale:

Customers should be aware of this default enablement so that they can account for enabled management interfaces.

Impact:

Lack of knowledge of enabled management interfaces can result in unexpected access of a network device.

Audit:

Customers can determine the state of the https-server through the following command:

```
switch# show https-server

HTTPS Server Configuration
-----

VRF                : default, mgmt
REST Access Mode   : read-write

Max sessions per user : 6

Session timeout      : 20
```

Remediation:

Customers that do not wish to have the https-server enabled can disable it using the following:

```
switch(config)# no https-server vrf <VRF-NAME>
```

Default Value:

AOS-CX campus switches have the https-server enabled on the default VRF. Products with an OOBM interface have the https-server enabled on the mgmt VRF.

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/rest_v10-0x/Content/Chp_ena_acc/https_serv_cmds/htt-ser-vrf-10.htm
2. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/rest_v10-0x/Content/Chp_ena_acc/https_serv_cmds/sho-htt-ser-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

1.9.2 https-server idle session management (Automated)

Profile Applicability:

- Level 1

Description:

https-server sessions are used by both the REST API and Web management interface (WebUI). By default, an https-server session will remain open for 20 minutes while idle. Customers should be setting the idle session timeout to the lowest value that can be tolerated.

Rationale:

The https-server session timeout impacts both the REST API and WebUI. If it's only the WebUI being used, then an idle timeout of 5 minutes is recommended. If the REST API is being used, then the timeout should be based on how the management system is using the REST API. Ultimately, setting the session timeout to the smallest value is recommended in order to address this threat.

Impact:

It's important that administrators know the idle duration of their management sessions. Sessions that are kept open too long may be taken over if the administrator walks away from their computer and fails to lock it. This can then lead to someone else gaining access to the device.

Audit:

The "show https-server" command displays the configured session timeout:

```
switch# show https-server

HTTPS Server Configuration
-----

VRF                : default, mgmt
REST Access Mode   : read-write

Max sessions per user : 6

Session timeout     : 20
```

Remediation:

The session-timeout option can be used to set the idle session timeout:

```
switch(config)# https-server session-timeout <minutes>
```

Default Value:

The https-server session timeout is set to 20 minutes by default.

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/rest_v10-0x/Content/Chp_ena_acc/https_serv_cmds/http-ser-ses-tim.htm
2. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/rest_v10-0x/Content/Chp_ena_acc/https_serv_cmds/sho-htt-ser-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

1.9.3 Two-factor authentication with the https-server server (Automated)

Profile Applicability:

- Optional Security Recommendations

Description:

Two-factor authentication provides an additional level of security by requiring administrators to perform X.509 certificate-based authentication with the AOS-CX https-server. The two factors are possession of the certificate private key and knowledge of the password associated with the certificate private key.

The switch must be configured with the corresponding CA certificate which issued the administrator's certificate.

Rationale:

Customers with a large number of administrators can be configuration and maintenance challenge across a large network. Use of certificate-based and two-factor authentication can simplify this maintenance for customers.

Impact:

Any changes in administrator user passwords or the additional or removal of administrator accounts can become a maintenance headache for customers. Use of two-factor authentication only requires the enablement of the feature and the addition of the corresponding CA certificate as a trust anchor.

Audit:

Two factor authentication configuration can be checked using the "show https-server authentication" command:

```
switch# show https-server authentication
```

```
Authentication Modes Status
```

```
-----
```

```
Password Status           : disabled
```

```
Certificate Status        : enabled
```

Trust Anchor (TA) profiles can be viewed using the "show crypto pki ta-profile" command:

```
switch(config)# show crypto pki ta-profile
TA Profile Name          TA Certificate          Revocation Check
-----
root-ca-for-ssh-server   Installed, valid        disabled
switch(config)#
```

Remediation:

```
switch(config)# https-server authentication certificate authorization radius
username common_name
```

Default Value:

Certificate-based authentication with the https-server is disabled by default.

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/rest_v10-0x/Content/Chp_ena_acc/https_serv_cmds/htt-ser-aut-cer.htm
2. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/rest_v10-0x/Content/Chp_ena_acc/https_serv_cmds/sho-htt-ser-aut.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 <u>Require MFA for Externally-Exposed Applications</u> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.			
v7	16.3 <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

1.9.4 Assign a custom certificate to the https-server (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

The https-server is enabled by default and is assigned the "local-cert" as its server certificate. The "local-cert" is a self-signed certificate generated internally by the switch at first boot. Self-signed certificates generally aren't trusted by browsers and shouldn't be used in normal operation. It is recommended that customers add their own server certificate to the switch and assign it to the https-server.

Rationale:

Self-signed certificates are normally flagged as invalid by modern browsers. The auto-generated "local-cert" serves as a placeholder for all certificate-based applications and is not meant for use in production networks.

Impact:

Use of the "local-cert" may result in the inability for clients to connect to the https-server. Or it will raise support calls as the authenticity of the device cannot be properly validated.

Audit:

The "show crypto pki application" command is used to view the certificate used by the https-server:

```
switch# show crypto pki application
```

Associated Applications	Certificate Name	Cert Status
-----	-----	-----

https-server		not configured, using local-
cert		
syslog-client	my-server-cert	valid
hsc		not configured, using local-
cert		
radsec-client	my-server-cert	valid

Remediation:

The 'crypto pki application' command can be used to assign a certificate to the https-server:

```
switch(config)# crypto pki application https-server certificate <CERT-NAME>
```

Default Value:

The https-server uses the auto-generated self-signed "local-cert" by default.

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Chp_PKI/ins-ca-sig-lea-cer-ini-swi-10.htm
2. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Chp_PKI/PKI_cmds/cry-pki-app-10.htm
3. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/security_5420-6200-6300-6400/Content/Chp_PKI/PKI_cmds/sho-cry-pki-app-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

1.10 Enable ServiceOS Password Authentication

Enabling ServiceOS Password Authentication ensures only privileged users can access the ServiceOS shell.

1.10.1 ServiceOS Password (Automated)

Profile Applicability:

- Level 1

Description:

This sequence describes enabling password authentication for ServiceOS login.

Rationale:

By default, the ServiceOS shell (accessible only from the local switch console port) requires no password to login as admin. This will allow un-privileged users with console access to log in to the ServiceOS shell.

Impact:

Enabling ServiceOS password authentication prevents unintended users from log into the ServiceOS shell, significantly reducing the risk of various security vulnerabilities and attacks.

Audit:

```
switch(config)# show system serviceos password-prompt
```

Remediation:

Enable ServiceOS password authentication:

```
switch(config)# system serviceos password-prompt
```

Default Value:

ServiceOS password authentication is disabled by default.

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/hardening/Content/Chp_hard-mgmt/serviceos-pwd-auth.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			
v8	<u>5.2 Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	<u>4.2 Change Default Passwords</u> Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.			
v7	<u>4.4 Use Unique Passwords</u> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

1.11 Securing Syslog

1.11.1 Assign a custom certificate to syslog-client (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

Syslog-client will default to using the "local-cert". The "local-cert" is a self-signed certificate generated internally by the switch at first boot.

Rationale:

The syslog-server can enforce more stringent checks on the syslog-client if both share a trusted certificate authority

Impact:

Use of the "local-cert" may result in the inability of the syslog-client to form a TLS connection to the syslog-server.

Audit:

The "show crypto pki application" command is used to view the certificate used by the syslog-client:

```
switch(config)# show crypto pki application
```

Associated Applications	Certificate Name	Cert Status
-----	-----	-----

captive-portal		not configured, using
local-cert		
dot1x-supPLICant		not configured, using
local-cert		
est-client		not configured, using
local-cert		
https-server		not configured, using
local-cert		
radsec-client		not configured, using
local-cert		
syslog-client	my-syslog-cert	invalid, using local-
cert		

Remediation:

The 'crypto pki application' command can be used to assign a certificate to the syslog-client:

```
switch(config)# crypto pki application syslog-client certificate <CERT-NAME>
```

Default Value:

The syslog-client uses the auto-generated self-signed "local-cert" by default.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

1.11.2 Configure syslog-client to log using TLS (Automated)

Profile Applicability:

- Optional Security Recommendations

Description:

Logging to a remote syslog server should be configured to use TLS and include auditable events.

Rationale:

Logging to a remote syslog server offers several advantages, including centralized log management, improved security, long-term data retention, and enhanced troubleshooting capabilities. By consolidating logs from various devices into a single location, administrators can easily monitor, analyze, and respond to issues across the network.

Impact:

Without a centralized logging location, logs on the switch may roll over and be lost.

Audit:

```
switch# show run | i logging
logging syslog.domain.tld tls 514 auth-mode subject-name vrf mgmt include-
auditable-events
```

Remediation:

Configure the switch to send logs to a syslog-server using tls on the mgmt VRF and include auditable events.

```
logging <SYSLOG-SERVER> tls <PORT> auth-mode subject-name vrf mgmt include-
auditable-events
```

Default Value:

sending logs to a syslog-server is not configured by default.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

1.12 Login Banner (Automated)

Profile Applicability:

- Level 1

Description:

Setting a banner to be displayed during the login process notifies users that unauthorized use is prohibited, and that access to and use of the system may be monitored and logged.

Rationale:

Login Banner serves as a compliance measure with legal requirements, alerting users about usage terms or unauthorized access penalties

Impact:

Login banner enhances security awareness, reinforces accountability, and ensures clarity in user interactions with the network device.

Audit:

To view the banner configurations -

Post Login Banner -

```
switch# show banner exec
```

Message of the Day Banner (Pre-Login) -

```
switch# show banner motd
```

Remediation:

To configure Message of the Day (Pre-Login) Banner -

```
switch(config)# banner motd <delimiter>  
switch(config)# <Banner Text> <delimiter>
```

To configure Post-Login Banner -

```
switch(config)# banner exec <delimiter>  
switch(config)# <Banner Text> <delimiter>
```

Sample Configuration of pre-login banner (motd) -

```

switch(config)# banner motd ^
Enter a new banner. Terminate the banner with the delimiter you have chosen.
switch(config-banner-motd)# This system is for authorized use only.
Unauthorized or improper
switch(config-banner-motd)# use of this system may result in civil or
criminal penalties. By
switch(config-banner-motd)# continuing to use this system you acknowledge
your consent to
switch(config-banner-motd)# these conditions of use.
switch(config-banner-motd)# ^

```

Sample Configuration of post-login banner -

```

switch(config)# banner exec ^
switch(config-banner-exec)# This banner is displayed after login
switch(config-banner-exec)# ^

```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/fundamentals_6300-6400/Content/Chp_IniCfg/cnf-ban.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

1.13 Schedule Configuration Backup Job (Automated)

Profile Applicability:

- Level 1

Description:

Create a job to periodically backup the configuration to a remote server.

Rationale:

It is crucial to have remote backups of configuration files for several key reasons, especially in today's digital landscape:

1. Disaster Recovery and Business Continuity:

- **Protection Against Local Disasters:** If your primary location experiences a disaster like fire, flood, or theft, having remote backups ensures your configuration files are safe and accessible from a different location.
- **Rapid Recovery:** Remote backups allow you to restore systems quickly after a disaster, minimizing downtime and ensuring business continuity.
- **Part of a Comprehensive Plan:** Remote backups are an essential component of a disaster recovery plan (DRP) and business continuity strategy.

2. Data Security and Redundancy:

- **Cyberattack Protection:** Remote backups provide an extra layer of security, especially against ransomware and other cyber threats. If your primary systems are compromised, you can restore from clean backups.
- **Protection Against Hardware Failure and Human Error:** Remote backups help you recover quickly from data loss due to hardware malfunctions, accidental deletions, or other human errors.
- **Geographical Redundancy:** Storing backups in different locations protects against localized disruptions.

3. Operational Benefits:

- **Automated Backups:** Remote backup services can be configured to run automatically, reducing manual effort and minimizing the risk of human error.
- **Scalability:** Remote backup solutions, particularly cloud-based ones, offer scalability to accommodate increasing data storage needs.
- **Remote Access:** You can access and restore your configuration files from anywhere with an internet connection, providing flexibility.

4. Compliance and Long-Term Preservation:

- Meeting Regulatory Requirements: Some industries and regulations mandate the use of offsite backups for data retention and compliance purposes.
- Long-Term Preservation: Remote backups help ensure the long-term preservation of data assets, safeguarding against corruption, hardware obsolescence, and technological advancements.

Impact:

If no remote configuration backup strategy is implemented you can be exposed to issues with business continuity, disaster recovery and compliance.

Audit:

check which jobs are configured:

```
switch# show job

Job Name : backup_config

Enabled           : Yes
Description       :
Status            : waiting
Number of commands : 1
Total execution count : 0
Failed execution count : 0

Job CLI commands
-----
1 cli copy running-config tftp://192.168.0.100/switch.cfg cli vrf mgmt
```

Check schedule of jobs:

```

switch# show schedule

Schedule Name: backup_config

Schedule config
-----
Description      :
Enabled          : Yes
Trigger type     : periodic
Transient        : No
Max trigger count : indefinite
Trigger start date : 2025-12-01 10:00

Schedule Status
-----
Trigger status   : active
Next trigger time : Mon Dec 1 10:00:00 2025

Scheduled Jobs
-----
1 : backup_config

```

Remediation:

Create a job to backup the configuration to a remote server

```

switch(config)# job backup_config
switch(config-job-config_backup)# 1 cli copy running-config
tftp://192.168.0.100/switch.cfg cli vrf mgmt

```

Schedule the job to run periodically:

```

switch(config)# schedule backup_config
switch(config-scheduler-backup_config)# 1 job backup_config
switch(config-scheduler-backup_config)# trigger every days 1 start 12:04
2024-03-18
switch(config-scheduler-backup_config)# enable
switch(config-scheduler-backup_config)# exit

```

Default Value:

No Jobs or Schedule configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.2 Perform Automated Backups Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.			

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.4 <u>Establish and Maintain an Isolated Instance of Recovery Data</u> Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.			
v7	10.1 <u>Ensure Regular Automated Back Ups</u> Ensure that all system data is automatically backed up on regular basis.			
v7	10.2 <u>Perform Complete System Backups</u> Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.			
v7	10.5 <u>Ensure Backups Have At least One Non-Continuously Addressable Destination</u> Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.			

1.14 Create Hostname (Automated)

Profile Applicability:

- Level 1

Description:

The host-name property should be set up to be unique name on the management network. This enables the switch to be resolved with a unique FQDN.

Rationale:

Device Management

- In networks with multiple switches, a unique hostname makes it easy to identify each device quickly.
- Avoids confusion when managing logs, alerts, and configurations.

Simplifies Management

- Hostnames appear in CLI prompts, SNMP, syslog messages, and monitoring tools.
- Easier for network admins to know which device an event or alert refers to.

Integration with Network Services

- Hostnames can be used in DNS for name resolution.
- Helpful when using automation tools

Compliance and Documentation

- Many organizations require meaningful hostnames for inventory and audit purposes.
- Supports naming conventions tied to location, function, or role.

Troubleshooting

- When reviewing logs or alerts, a clear hostname reduces errors and speeds up root cause analysis.

Audit:

```
show running-configuration | hostname
```

Remediation:

```
switch(config)# hostname _[name]_
```

2 Interface

Interface level security in HPE ANW CX switches ensures secure access and protects against threats by safeguarding both physical and virtual interfaces. This section will cover features that handles security in the interface level

2.1 Physical Security

2.1.1 Disable USB and Bluetooth on Device (Automated)

Profile Applicability:

- Level 2

Description:

Disable USB Auxiliary port

Rationale:

The AOS-CX switch front-panel includes an USB Auxiliary port for the following purposes:

- USB Mass storage - flash drive for deploying, troubleshooting, backing up configurations, or upgrading switches
- Bluetooth Adapter - allows Bluetooth enabled devices to connect to and manage the switch on a wireless Bluetooth Personal Area Network (PAN)

The Bluetooth feature has been enabled by default in AOS-CX switches and designed for operational simplicity. The switch provides an IP address to paired devices though DHCP when they join the Bluetooth Personal Area Network. Paired devices can then manage the switch through following methods:

- SSH
- Web UI
- REST API
- Aruba CX Mobile App

Impact:

Disabling USB will prevent both USB devices from being mounted and Bluetooth adapters from being enabled.

Disabling Bluetooth will only prevent Bluetooth adapters from being enabled.

Audit:

Check the status of USB

```
switch# show usb
```

Check the status of Bluetooth

```
switch# show bluetooth
```

Remediation:

```
switch(config)# no usb  
switch(config)# bluetooth disable
```

Default Value:

- USB: Enabled
- Bluetooth: Enabled

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/fundamentals_6300-6400/Content/SysHW_cmds/usb-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.9 <u>Encrypt Data on Removable Media</u> Encrypt data on removable media.			
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	13.7 <u>Manage USB Devices</u> If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.			
v7	15.9 <u>Disable Wireless Peripheral Access of Devices</u> Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.			

2.1.2 Front Panel Security (Manual)

Profile Applicability:

- Level 1

Description:

This sequence describes auditing the front panel reset button status

Rationale:

AOS-CX switches include a reset button on the front panel to allow users to perform the following reset operations:

Reset Type	Procedure	Outcome
Soft Reset	Press the reset button and release it before 5 seconds.	The switch operating system is cleared gracefully. The switch then reboots and runs self-tests.
Hard Reset	Press the reset button and release it between 5 to 20 seconds.	The switch reboots, like a power cycle. A hard reset is used, for example, when the switch CPU is in an unknown state or not responding.
Factory Reset	Press the reset button and release it between 20 to 25 seconds.	The switch will undergo the factory reset process.

Impact:

This factory reset capability creates a security and denial-of-service risk if the switch is in a location where it is impossible to prevent physical access to the front panel. It is disabled by default and recommended that administrators disable this feature after its usage to prevent malicious use by an attacker with physical access to the device.

Audit:

To display front panel reset button status:

```
switch# show front-panel-security status
Front panel factory reset           : disabled
First occurrence of front-panel factory reset : N/A
```

Remediation:

n/a

Default Value:

The front panel reset button is disabled by default

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/hardening/Content/Chp_hard-mgmt/phys-secur.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.1.3 Disable Unused Physical Interfaces (Manual)

Profile Applicability:

- Level 1

Description:

Disable unused physical interfaces.

Rationale:

Unused physical interfaces could allow an attacker to plug in a network cable and access network resources (depending on the configuration of that port).

Impact:

Disabling unused physical interfaces helps to:

- Reduce the attack surface by minimizing open entry points, thus reducing pathways for attackers to access your network.
- Prevent unauthorized network access.
- Ensure compliance with many regulatory standards that require only necessary network ports to be active to maintain a secure environment.
- Improve network hygiene by regularly managing and configuring port settings.
- Enhance incident response by making it easier to isolate and respond effectively to security breaches with fewer active ports.

Audit:

Check which physical interfaces are enabled:

```
switch# show interface physical
```

Remediation:

Disable unused physical interfaces

```
switch# conf
switch(config)# interface 1/1/1
switch(config-if)# shutdown
switch(config-if)#
```

Default Value:

On AOS-CX switches 8XXX,9XXX,1XXXX physical interfaces are disabled by default, rest of the switches in AOS-CX portfolio have physical interfaces enabled by default.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.12 <u>Segment Data Processing and Storage Based on Sensitivity</u> Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.			
v8	3.13 <u>Deploy a Data Loss Prevention Solution</u> Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			
v7	14.1 <u>Segment the Network Based on Sensitivity</u> Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).			
v7	14.7 <u>Enforce Access Control to Data through Automated Tools</u> Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.			

2.2 Traffic Control - Rate limiting (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

Configuring rate-limiting on Aruba CX switches allows administrators to control the maximum amount of traffic (bandwidth) that can pass through specific interfaces or for specific traffic types. This ensures that no single device or application can consume excessive network resources. Specifies the type of ingress traffic to which the rate limit applies: broadcast, multicast, unknown-unicast, or ICMP. The multicast rate limit affects multicast and broadcast traffic. The broadcast rate limit only affects broadcast traffic. When both types are applied to the same interface, broadcast packets are limited to the lower of the two rate values. Layer 2 BPDU packets, like spanning tree, are also included in the multicast rate limit. The ICMP rate limit can be configured to apply to IPv4, IPv6, or all IP traffic. Only one ICMP rate-limit can be configured at a time. Applying a new ICMP rate-limit replaces any previous ICMP rate-limit.

Specifies the rate limit in kilobits per second, packets per second, or as a percentage of link bandwidth. Range: 64 to 100000000 kbps (in steps of 64 kbps), 64 to 209090910 pps (in steps of 64 pps), or 1-100 percent. The actual rate limit will be approximately equivalent to the minimum of the two step values that are closest to the configured rate (or for percent mode, the kbps-converted rate).

Rationale:

Rate-limiting is implemented to prevent network congestion, mitigate the impact of potential denial-of-service (DoS) attacks, and ensure fair bandwidth allocation among users and applications. It helps maintain optimal network performance and stability.

Impact:

By configuring rate-limiting, organizations can improve network efficiency, protect critical services from being overwhelmed by excessive traffic, and ensure a consistent user experience. This proactive measure enhances both security and operational reliability.

Audit:

To view the configuration change -

```
switch# show interface <interface-ID> qos
```

Sample results -

```

switch# show interface 1/1/3 qos
Interface 1/1/3 is up
Admin state is up
Description:
Hardware: Ethernet, MAC Address: 08:97:34:b1:20:00
MTU 1500
Type 1000BT
qos trust none
rate-limit broadcast 2000 pps (2000 actual)
rate-limit icmp ip-all 10000 kbps (10000 actual)
Speed 1000 Mb/s
L3 Counters: Rx Disabled, Tx Disabled
Auto-Negotiation is on
Flow-control: off
Rx
      0 input packets          0 bytes
      0 input error            0 dropped
      0 CRC/FCS
L3:
      0 packets, 0 bytes
Tx
      127 output packets       16510 bytes
      0 input error            0 dropped
      0 collision
L3:
      0 packets, 0 bytes

```

Remediation:

To configure rate-limit in interfaces -

```

switch(config)# interface <ID>
switch(config)# rate-limit {broadcast|multicast|unknown-unicast|icmp {ip-
all|ip|ipv6}} <RATE> {kbps|percent|pps}

```

Sample configurations -

Limiting broadcast traffic to 2000pps on interface 1/1/3:

```

switch(config)# interface 1/1/3
switch(config-if)# rate-limit broadcast 500 kbps

```

Limiting all ICMP IPv4 traffic to 10000kbps on interface 1/1/3:

```

switch(config)# interface 1/1/3
switch(config-if)# rate-limit icmp ip 10000 kbps

```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/qos_5420-6200-6300-6400/Content/Chp_Config/cnf-rat-lim-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

2.3 Proxy ARP (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

Proxy ARP is a technique by which a device on a given network answers the ARP queries for a network address that is not on that network. The ARP proxy is aware of the location of the traffic's destination, and offers its own MAC address as the final destination. Proxy ARP is supported on L3 physical and VLAN interfaces. It is disabled by default. Disabling Proxy ARP on unused interfaces in AOS-CX switches prevents the switch from responding to ARP requests on behalf of other devices, ensuring that it does not act as a proxy for IP address resolution on inactive ports.

Rationale:

Enhances network security by preventing potential misuse of unused interfaces, such as spoofing or unauthorized traffic redirection. It also reduces unnecessary processing and ARP-related traffic on the network.

Impact:

Disabling Proxy ARP on unused interfaces minimizes attack surfaces, safeguards against ARP-based attacks, and contributes to an optimized and secure network environment by eliminating unnecessary overhead on inactive ports.

Audit:

All interfaces have the proxy arp capability turned off by default. To make sure it's not enabled, the show command below can be verified. IPv4 -

```
switch# show run | in proxy-arp
```

IPv6 -

```
switch# show run | in proxy-nd
```

Remediation:

Proxy ARP is disabled on all interfaces by default. Proxy ARP appears in the configuration only if it is enabled (which is usually undesirable). Disable this on an interface if it is enabled using below Configuration -

```
switch(config)# interface <ID>
switch(config)# no ip proxy-arp
switch(config)# no ip local-proxy-arp
switch(config)# no ipv6 local-proxy-nd
```

Default Value:

Proxy-arp is disabled by default on all the vlan interfaces

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/ip_services_6300-6400/Content/Chp_ARP/ARP_cmds/ip-pro-arp.htm
2. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/ip_services_6300-6400/Content/Chp_ARP/ARP_cmds/ip-loc-pro-arp.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.4 IP Directed Broadcast (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

IP Directed Broadcast is a feature by which remote administration tasks such as backups and wake-on-LAN (WOL) application can be achieved by sending directed broadcast packets for hosts and servers residing on a different subnets. IP Directed Broadcast is supported on ROP, SVI and L3LAG interfaces. It is disabled by default. Disabling IP directed broadcast on unused interfaces in AOS-CX switches prevents the switch from converting directed broadcast packets into Layer 2 broadcasts on a destination subnet. This configuration ensures that such traffic is dropped rather than propagated further into the network.

Rationale:

IP directed broadcasts are often exploited in amplification attacks, such as Smurf attacks, which flood the network with broadcast traffic to disrupt operations. By disabling this feature on unused interfaces, network administrators can reduce the likelihood of these types of exploits. Additionally, it prevents unnecessary broadcast traffic from consuming resources on unused subnets.

Impact:

Disabling IP directed broadcast on unused interfaces enhances network security by mitigating potential DoS amplification attacks. It reduces unnecessary processing and bandwidth usage caused by broadcast traffic on inactive interfaces. This configuration helps maintain network stability, improves overall performance, and minimizes attack surfaces by reducing the exposure of unused interfaces to malicious activity.

Audit:

IP Directed Broadcast is disabled by default , it can be validated using below show command -

```
switch# show run | in "ip directed-broadcast"
```

Remediation:

IP Directed broadcast is disabled by default on all interface , to disable it incase if its enabled by mistake -

```
switch(config)# interface <ID>
switch(config)# no ip directed-broadcast
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/ip_route_6300-6400-8100-83xx-9300-10000/Content/Chp_IPDirBroad/ip-dir-bro55.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			
v7	12.4 <u>Deny Communication over Unauthorized Ports</u> Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.			

3 Protocol

Protocol security in HPE ANW CX switches focuses on protecting network communication protocols from exploitation, ensuring secure and reliable data transmission. HPE ANW CX switches include features to safeguard critical protocols such as ARP, DHCP, and routing protocols, which are often targeted in spoofing and injection attacks. This section cover the guidelines to protect the protocols.

3.1 Routing Protocols

The following sections describe the workflows for securing OSPF and BGP routing protocols.

3.1.1 OSPF

3.1.1.1 OSPF Passive Interfaces (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

Enable OSPF Passive Interfaces

Rationale:

The OSPF Passive Interface feature is used to prevent OSPF from forming neighbor relationships or exchanging Hello packets on specified interfaces, while still allowing the connected subnet to be advertised in the OSPF routing domain. This enhances network security by avoiding unauthorized OSPF adjacencies, reduces unnecessary control traffic, and optimizes resource utilization by limiting OSPF operations to only required interfaces. It is particularly useful for interfaces connected to end-user devices or untrusted networks, improving network stability and simplifying management

Impact:

To limit where OSPF can learn neighbors, AOS-CX supports the passive OSPF interfaces. A passive OSPF interface has its IP subnets announced, but it does not establish neighbor relationships with other OSPF devices on the interface. You must make all OSPF enabled interfaces passive. Setting the OSPF enabled interfaces to from default to passive is done in the OSPF router instance context. The passive interface is then removed from each interface where OSPF neighbor relationships are allowed. Since this is an interface-level configuration change, it can be done from the interface context

Audit:

To view the OSPF Passive interface configurations -

OSPF -

```
switch# show ip ospf [<process-id>] [all-vrfs | vrf <vrf-name>]  
switch# show ip ospf interface <interface-ID>
```

OSPFv3 -

```
switch# show ipv6 ospfv3 [<process-id>] [all-vrfs | vrf <vrf-name>]  
switch# show ipv6 ospfv3 interface <interface-ID>
```

Remediation:

Configure all OSPF enabled interfaces to be passive in OSPF router context

OSPF -

```
switch(config)# router ospf <OSPF Process ID>
switch(config-ospf-<Process ID># passive-interface default
```

OSPFv3 -

```
switch(config)# router ospfv3 <OSPF Process ID>
switch(config-ospfv3-<Process ID># passive-interface default
```

The passive interface is then removed from each interface where OSPF neighbor relationships are allowed. Since this is an interface-level configuration change, it can be done from the interface context:

To disable passive interface from selective interfaces -

OSPF -

```
switch(config)# interface <interface ID>
switch(config-if)# no ip ospf passive
```

OSPFv3 -

```
switch(config)# interface <interface ID>
switch(config-if)# no ipv6 ospfv3 passive
```

Default Value:

Not Set

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/ip_route_6300-6400-8100-83xx-9300-10000/Content/Chp_OSPFv2/OSPFv2_cmds/pas-int-def.htm
2. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/ip_route_6300-6400-8100-83xx-9300-10000/Content/Chp_OSPFv3/OSPFv3_cmds/pas-int-osp.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.12 Segment Data Processing and Storage Based on Sensitivity Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.		●	●
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	12.4 <u>Deny Communication over Unauthorized Ports</u> Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.			
v7	14.1 <u>Segment the Network Based on Sensitivity</u> Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).			

3.1.1.2 OSPF Neighbor Authentication (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

Enable OSPF Neighbor Authentication

Rationale:

The purpose of configuring OSPF neighbor authentication is to secure communication between OSPF routers and protect the integrity of routing information exchanged. By default, OSPF uses "null" authentication, meaning no authentication is applied, leaving OSPF control packets vulnerable to unauthorized access, tampering, or injection of malicious routing information. Introducing cryptographic authentication methods, such as HMAC-SHA-512, ensures that OSPF neighbors exchange routing information securely, preventing unauthorized devices from becoming OSPF neighbors and mitigating risks such as routing table poisoning or network disruptions caused by malicious actors.

Impact:

HMAC-SHA-512 is a robust cryptographic hashing algorithm that offers strong protection against brute force and collision attacks. Configuring SHA-512 ensures a higher level of security for OSPF communications compared to plaintext passwords or weaker hashing algorithms. Requiring both devices to use the same authentication method and key ensures consistency and interoperability between OSPF neighbors, which is critical for maintaining stable OSPF adjacencies

Audit:

To view the OSPF neighbor authentication in interface -

```
switch# show ip ospf interface <interface-ID>
```

Remediation:

AOS-CX keychain feature can be used to specify a system-level cryptographic authentication key which can be used by multiple OSPF interfaces -

To configure the keychain with HMAC-SHA-512 cryptographic algorithm and keystore (Keystore can be entered as plaintext or as a hashed ciphertext string)-

```
switch(config)# keychain <keychain-name>
switch(config-keychain)# key <ID>
switch(config-keychain-key)# cryptographic-algorithm hmac-sha-512
switch(config-keychain-key)# key-string plaintext <plaintext-key-string>
```

To associate the keychain in the OSPF enabled interface -

```
switch(config-keychain-key)# interface <interface-ID>
switch(config-if)# ip ospf authentication keychain
switch(config-if)# ip ospf keychain <keychain-name>
```

Default Value:

Not Set

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/ip_route_6300-6400-8100-83xx-9300-10000/Content/Chp_OSPFv2/OSPFv2_cmds/ip-osp-aut-10-59.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

3.1.1.3 OSPFv3 Area Authentication and Encryption with IPsec (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

OSPFv3 neighbors may use interface-level authentication. An alternative method might be used to provide encryption, or authentication, or both for an entire OSPFv3 area using the IPsec protocol, which automatically applies the configured methods to all member interfaces. There are two IPsec encapsulation types supported on AOS-CX to secure OSPFv3 areas:

- IPv6 authentication header (AH), which adds an IPv6 authentication header to OSPFv3 packets.
- Encrypted Security Payload (ESP), which provides both authentication and encryption for OSPFv3 packets.

Rationale:

The implementation of OSPFv3 (Open Shortest Path First version 3) Area Authentication and Encryption using IPsec is essential for enhancing the security of routing protocols in modern networks. OSPFv3 is widely used in IPv6 environments, and its reliance on trust between routers makes it vulnerable to attacks such as unauthorized route injection, replay attacks, or data interception. By integrating IPsec for authentication and encryption, network administrators can ensure that OSPFv3 exchanges are securely transmitted, protecting the integrity and confidentiality of routing information. This added layer of security prevents malicious actors from compromising the routing infrastructure, thereby maintaining the reliability and performance of the network.

Impact:

The use of IPsec for OSPFv3 authentication and encryption significantly strengthens the security posture of networks by safeguarding routing updates in transit. This ensures that only authorized routers can participate in OSPFv3 exchanges and that all routing information remains confidential and tamper-proof. As a result, the risk of routing table manipulation, traffic redirection, and denial of service attacks is greatly reduced. Furthermore, the adoption of IPsec aligns with organizational compliance requirements and best practices for securing IPv6 networks, mitigating vulnerabilities associated with unprotected routing protocols. Ultimately, this approach enhances network stability, reduces downtime, and fosters trust in critical communication infrastructure.

Audit:

To view the configuration change -

```
show run ospfv3
show ipv6 ospfv3 [<process-id>] [all-vrfs | vrf <vrf-name>]
```

Remediation:

IPsec authentication and encryption are configured from the OSPFv3 router process context. Both authentication and encryption require a specified Security Policy Index (SPI), which is an integer value between 256 and 4,294,967,295; this value is used on each OSPFv3 router in the secured area to match a configured IPsec authentication and/or encryption policy. Each OSPFv3 IPsec policy on a switch must use a different SPI value, and the SPI value (as well as authentication, or encryption keys, or both) must match across all OSPFv3 neighbor interfaces using that policy within the secured area. To configure AH authentication for OSPFv3 area 1, specify the SPI, authentication method (md5 or sha1), key type (plaintext, hex-string, or ciphertext) and the key string itself. If a key type and string are not specified, the user is prompted to enter a plaintext key interactively:

```
switch(config)router ospfv3 <process-ID>
switch(config-ospfv3-<process>)# area 1 authentication ipsec spi 1024 sha1
Enter the IPsec authentication key: *****
Re-Enter the IPsec authentication key: *****
```

To configure ESP encryption for area 1, specify the SPI, authentication method, authentication key type and string, encryption type (3des, aes, des, or null), key type, and encryption key string. If the encryption type and key string are not specified, you are prompted to enter a plaintext key interactively. If the authentication key type and string are not specified, you are prompted to enter both a plaintext authentication key as well as the desired encryption type and plaintext key.

```
switch(config)router ospfv3 <process-ID>
switch(config-ospfv3-<process>)# area 1 encryption ipsec spi 1024 sha1
Enter the IPsec authentication key: *****
Re-Enter the IPsec authentication key: *****
Enter the IPsec encryption type (3des/aes/des/null)? aes
Enter the IPsec encryption key: *****
Re-Enter the IPsec encryption key: *****
```

Depending on the selected encryption type, a plaintext or hexadecimal encryption key must be set to a specific length as mentioned below:

- 3DES:
 - Hexadecimal: 48 digits
 - Plaintext: 24 characters
- DES:
 - Hexadecimal: 16 digits
 - Plaintext: 8 characters
- AES:
 - Hexadecimal: 32, 48, or 64 digits
 - Plaintext: 16, 24, or 32 characters

For AES encryption, the specified key lengths correspond to AES128, AES192, or AES256, respectively; the type of the key that will be used is automatically determined by the length of the entered encryption key. AOS-CX recommends using AES over DES or 3DES as it is stronger.

Default Value:

No Default Value Set

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/ip_route_6300-6400-8100-83xx-9300-10000/Content/Chp_OSPFv3/OSPFv3_cmds/are-aut-ips-osp-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

3.1.2 BGP

This section covers the best practices to secure BGP protocol.

The IETF Best Current Practices for BGP Security (BCP194) focuses on the following three items:

- Utilizing the control-plane ACL functionality to limit BGP communication to configured BGP peers.
- Securing BGP sessions between peers by using authentication.
- Use TTL Security Mechanisms to prevent spoofing attacks from third parties.

3.1.2.1 Control Plane ACL for BGP Peering Sessions (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

Utilizing the control-plane ACL functionality to limit BGP communication to configured BGP peers

Rationale:

Control Plane ACLs (CP-ACLs) are essential for securing BGP peering sessions by restricting unauthorized access to the control plane. They prevent threats like spoofed packets, unauthorized session attempts, and malicious traffic, ensuring only legitimate BGP traffic is processed. This protects the routing infrastructure's stability and prevents vulnerabilities

Impact:

Implementing CP-ACLs enhances network security and stability by safeguarding the control plane from attacks such as DDoS or unauthorized BGP manipulation. This ensures secure and reliable routing updates, reduces disruptions, and strengthens the overall resilience and trustworthiness of the routing infrastructure.

Audit:

To view the control plane ACL configuration -

```
switch# show access-list control-plane
```

Remediation:

Devices running BGP listen for connections on TCP port 179. When establishing a BGP peer session, one device actively establishes a relationship with the other peer by sending the first TCP SYN packet. This device is at the outgoing side of the connection. The other peer, hearing the TCP SYN, responds with a SYN or ACK at the incoming connection. As each peer can assume either role, ACL entries need to be configured for BGP in both directions. Sample Control Plane ACL example is shown below, the these entries permit traffic from 10.20.0.10 so that it can establish a BGP peering session with the device. Either side could play the outgoing or incoming role in the BGP connection, so the ACL requires two entries per peer After allowing traffic from all configured peers, block all other devices from establishing a BGP peering session by denying all other traffic to or from TCP port 179.

```

switch(config)# access-list ip <CONTROLPLANE-ACL-NAME>
switch(config-acl-ip)# 800 comment LOCKDOWN BGP SESSIONS
switch(config-acl-ip)# 805 permit tcp <10.20.0.10> gt 1023 any eq 179
switch(config-acl-ip)# 810 permit tcp <10.20.0.10> eq 179 any gt 1023
switch(config-acl-ip)# 815 deny tcp any gt 1023 any eq 179
switch(config-acl-ip)# 820 deny tcp any eq 179 any gt 1023
switch(config-acl-ip)# 990 comment ALLOW ANYTHING ELSE
switch(config-acl-ip)# 1000 permit any any any
switch(config-acl-ip)# exit
switch(config) apply access-list {ip|ipv6} <CONTROLPLANE-ACL-NAME> control-
plane vrf <VRF-NAME>

```

Default Value:

No Default value set

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/acls_6300-6400-8100-8360/Content/Chp_ACLs/ACLs_cmds/app-acc-lis-con-pla.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

3.1.2.2 Authenticate BGP Peers Using MD5 (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

The TCP sessions between the two peers can be secured by adding MD5 protection to the TCP session header

Rationale:

Authenticating BGP peers using MD5 ensures that only trusted and authorized devices can establish BGP sessions, protecting the integrity of the routing infrastructure. By adding a cryptographic layer of authentication, MD5 mitigates risks such as session hijacking, spoofed connection attempts, or unauthorized access, ensuring that routing updates are exchanged securely between peers

Impact:

Using MD5 for BGP peer authentication significantly improves network security by preventing unauthorized devices from establishing BGP sessions. This reduces the risk of malicious activity, such as route injection or disruption of routing operations, ensuring reliable and secure communication between peers while maintaining the stability and trustworthiness of critical routing protocols.

Audit:

To view the BGP configuration -

```
switch# show run bgp
```

Remediation:

The TCP sessions between the two peers can be secured by adding MD5 protection to the TCP session header. The MD5 digest acts like a password between peers. This configuration is done within the BGP configuration context, and both peers need to configure the same password either plaintext or ciphertext.

```
switch(config)# router bgp <ASN>
switch(config-bgp)# neighbor {<IP-ADDR>|<PEER-GROUP-NAME>} password
[{ciphertext | plaintext} <PASSWORD>]
```

Default Value:

No Default Value Set

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/ip_route_6300-6400-8100-83xx-9300-10000/Content/Chp_BGP/BGP_cmds/nei-pas-10.87.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.			
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.			

3.1.2.3 BGP TTL Security (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

Enables BGP to establish connection with external peers residing on networks that are not directly connected

Rationale:

BGP TTL Security is designed to prevent unauthorized devices or attackers from establishing BGP sessions by leveraging the Time-to-Live (TTL) field in IP headers. By requiring BGP packets to have a specific TTL value, typically set high (e.g., 255), it ensures that only directly connected peers can communicate, blocking spoofed or malicious BGP traffic from distant sources.

Impact:

Implementing BGP TTL Security enhances the protection of BGP sessions by preventing attacks such as spoofed route advertisements or unauthorized session establishment from non-directly connected sources. This strengthens the network's resilience against threats, reduces the risk of routing instability, and ensures reliable, secure communication between legitimate BGP peers.

Audit:

To view the BGP configuration -

```
switch# show run bgp
```

Remediation:

Configuration to enable BGP neighbor ttl-security-hops -

```
switch(config)# router bgp <ASN>  
switch(config-bgp)# neighbor {<IP-ADDR>|<PEER-GROUP-NAME>} ttl-security-hops  
<hop-count>
```

Default Value:

No Default Value Set

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/ip_route_6300-6400-8100-83xx-9300-10000/Content/Chp_BGP/BGP_cmds/nei-ttl-sec-hop-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.12 <u>Segment Data Processing and Storage Based on Sensitivity</u> Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.			
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			
v7	12.4 <u>Deny Communication over Unauthorized Ports</u> Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.			
v7	14.1 <u>Segment the Network Based on Sensitivity</u> Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).			

3.2 DHCP Protocols

DHCP (Dynamic Host Configuration Protocol) plays a critical role in dynamically assigning IP addresses and other network configuration information to devices on a network. However, it is also a potential target for network attacks, such as rogue DHCP servers and IP address spoofing attacks. To mitigate these risks, Aruba AOS-CX switches include robust DHCP hardening protocols and security mechanisms. This section cover those protocols.

3.2.1 DHCP Snooping

DHCP snooping is a security feature that helps avoid problems caused by an unauthorized DHCP server on the network that provides invalid configuration data to DHCP clients. A user without malicious intent may cause this problem by unknowingly adding to the network a switch or other device that includes a DHCP server enabled by default. In some cases, a user with malicious intent adds a DHCP server to the network as part of their Denial of Service or Man in the Middle attack. DHCP snooping helps prevent such problems by distinguishing between trusted ports connected to legitimate DHCP servers and untrusted ports connected to general users. DHCP packets are forwarded between trusted ports without inspection. DHCP packets received on other switch ports are inspected before being forwarded. DHCP Packets from untrusted sources are dropped.

3.2.1.1 DHCPv4 & DHCPv6 Snooping Enablement (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

DHCP snooping protects the network from common DHCP attacks, including address spoofing resulting from a rogue DHCP server operating on the network or exhaustion of addresses on a DHCP server caused by mass address requests by an attacker on the network. DHCP snooping designates trusted DHCP servers and ports on which DHCP requests and responses are accepted.

Rationale:

DHCP Snooping classifies switch ports as either trusted or untrusted. Trusted ports are those connected to legitimate DHCP servers. Untrusted ports are typically edge ports connected to end devices or untrusted networks. The switch inspects DHCP messages and allows only valid responses from trusted ports. Malicious or unauthorized DHCP responses from untrusted ports are dropped.

Impact:

Prevents rogue DHCP servers from assigning incorrect or malicious IP configuration to clients. Protects against DHCP-based man-in-the-middle attacks.

Audit:

To view the configuration change with DHCPv4 & DHCPv6 snooping -

```
switch# show dhcpv4-snooping
switch# show dhcpv6-snooping
```

Remediation:

The following is a DHCPv4-snooping sample configuration -

```
switch(config)# dhcpv4-snooping
switch(config)# vlan <vlan-id>
switch(config-vlan-id)# dhcpv4-snooping
switch(config-vlan-id)# exit
switch(config)#
switch(config)# interface <trusted interface id>
switch(config-if)# dhcpv4-snooping trust
switch(config-if)# exit
switch(config)# dhcpv4-snooping authorized-server <ipv4-server-address> vrf
<vrf-name>
```

The following is a DHCPv6-snooping sample configuration:

```

switch(config)# dhcpv6-snooping
switch(config)# vlan <vlan-id>
switch(config-vlan-id)# dhcpv6-snooping
switch(config-vlan-id)# exit
switch(config)#
switch(config)# interface <trusted interface id>
switch(config-if)# dhcpv6-snooping trust
switch(config-if)# exit
switch(config)# dhcpv6-snooping authorized-server <ipv6-server-address> vrf
<vrf-name>

```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/ip_services_6300-6400/Content/Chp_DHCP_snoop/dhc-sno-fl-ml-xl-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.			
v8	7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.			
v8	13.5 Manage Access Control for Remote Assets Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>12.2 Scan for Unauthorized Connections across Trusted Network Boundaries</u> Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.			
v7	<u>12.4 Deny Communication over Unauthorized Ports</u> Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.			

3.2.1.2 DHCPv6 Guard (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

DHCPv6 guard is an extension of DHCPv6 snooping. When the DHCPv6 snooping feature is configured globally and on the VLAN, the ports are configured as trusted and untrusted ports. DHCPv6 guard enhances this by creating a policy and applying it on a port and on the VLAN. This policy contains multiple attributes which are compared against the packet that is received on trusted ports. If the packet complies with the attributes of the policy, it is forwarded to the destination port; otherwise the packet is dropped.

Rationale:

The DHCPv6 Guard feature on AOS-CX switches helps prevent rogue DHCPv6 servers from distributing unauthorized IPv6 addresses and configurations, ensuring the integrity of network operations. It achieves this by filtering DHCPv6 server messages on trusted ports.

Impact:

By mitigating the risks of rogue servers, DHCPv6 Guard enhances network security, reduces potential misconfigurations, and ensures reliable IPv6 address management, leading to a more stable and secure network infrastructure.

Audit:

To view the configuration change with DHCPv6 guard:

```
switch# show dhcpv6-snooping guard-policy
```

Remediation:

The following are sample configurations of DHCPv6 guard -

```

switch(config)# dhcpv6-snooping guard-policy <policy-name>
switch(config-dhcpv6-guard-policy)# match server access-list <acl-name>
switch(config-dhcpv6-guard-policy)# preference min <6>
switch(config-dhcpv6-guard-policy)# preference max <250>
switch(config-dhcpv6-guard-policy)# match client prefix-list <prefix-list>
switch(config-dhcpv6-guard-policy)# exit
switch(config)# vlan <vlan-id>
switch(config-vlan-id)# dhcpv6-snooping guard-policy <policy-name>

```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/ip_services_6300-6400/Content/Chp_DHCP_snoop/Dv6Snoop_cmds/dhcv6-sno-gua-pol.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.			
v8	7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.			
v8	13.5 Manage Access Control for Remote Assets Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	12.2 <u>Scan for Unauthorized Connections across Trusted Network Boundaries</u> Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.			
v7	12.4 <u>Deny Communication over Unauthorized Ports</u> Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.			

3.3 Multicast

3.3.1 PIM

In a network where IP multicast traffic is transmitted for multimedia applications, this traffic is blocked at routed interface (VLAN) boundaries unless a multicast routing protocol is running. Protocol Independent Multicast (PIM) is a family of routing protocols that form multicast trees to forward traffic from multicast sources to subnets that have used a protocol such as IGMP to request the traffic. In this section you will find features to harden PIM.

3.3.1.1 PIM Accept-Register (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

PIM Accept-register is a security feature designed to control which sources and groups are allowed to register with the Rendezvous Point (RP). This feature works alongside the RP configuration and includes an access list (ACL) option to filter sources and groups. The ACL specifies rules for permitting or denying traffic based on source and group addresses. When configured, this functionality ensures that only authorized multicast sources and groups are registered with the RP, enhancing security and preventing unauthorized multicast traffic.

Rationale:

By associating an ACL with a PIM router, administrators can filter and control the registration of multicast sources and groups. Without such control, unauthorized or malicious sources could register with the RP, potentially leading to resource misuse or network disruption. The PIM Accept-register feature performs a lookup to check if the source (S) and group (G) in a packet match the permitted list defined in the ACL. If there is no match or if a deny rule is encountered, the packet is dropped immediately, and a register stop message is sent. This mechanism ensures that only permitted multicast traffic is processed, enhancing the network's security and operational efficiency.

Impact:

Packets matching the ACL permit rules are processed normally, while denied or unmatched packets are immediately dropped with a register stop message sent. This prevents unauthorized or malicious traffic from reaching the RP, enhancing network security and efficiency.

Audit:

To view the configuration change -

```
switch# show run pim
switch# show run pim6
```

Remediation:

Sample PIM Accept-Register configuration -

```

switch(config)# access-list ip <pim_reg_acl>
switch(config-acl-ip)# 10 permit any <20.1.1.1> <225.1.1.2>
switch(config-acl-ip)# 20 deny any <30.1.1.1> <225.1.1.3>
switch(config-acl-ip)# exit
switch(config)# router pim
switch(config-pim)# accept-register access-list <pim_reg_acl>
switch(config-pim)# exit
switch(config)# access-list ipv6 <pim_regv6_acl>
switch(config-acl-ipv6)# 10 permit any <20::1> <ff1e::1>
switch(config-acl-ipv6)# 20 deny any <30::1> <ff1e::3>
switch(config-acl-ipv6)# exit
switch(config)# router pim6
switch(config-pim6)# accept-register access-list <pim_regv6_acl>
switch(config-pim6)# exit

```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/multicast_5420-6200-6300-6400-8xxx-9300-10000/Content/Chp_pim-sm/pim-sm-ipv4_cmds/acc-reg-acc-lis.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	3.13 Deploy a Data Loss Prevention Solution Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			
v7	14.7 Enforce Access Control to Data through Automated Tools Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.			

3.3.1.2 PIM Accept-RP (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

PIM Accept-RP allows administrators to restrict which multicast groups a rendezvous point (RP) serves in a PIM sparse mode domain. By default, an RP accepts all multicast groups in the 224.0.0.0/4 range. Using an access list (ACL), this feature limits join/prune message processing to specific multicast groups, enhancing control and reducing unnecessary traffic.

Rationale:

Without restrictions, an RP processes join/prune messages for all multicast groups in the default Class D range, leading to potential resource waste and security risks. PIM Accept-RP, configured with an ACL, ensures the RP handles only authorized multicast groups, preventing unwanted traffic and optimizing network operations.

Impact:

The feature improves multicast efficiency and security by filtering out unauthorized groups. Permitted groups are processed as usual, while unwanted traffic is ignored. This targeted control reduces resource consumption and limits the risk of malicious or unnecessary multicast activity.

Audit:

To view the configuration change -

```
switch# show run pim
switch# show run pim6
```

Remediation:

Configuration to enable PIM Accept RP ACL -

```

switch(config)# access-list ip <pim_rp_grp_acl>
switch(config-acl-ip)# 10 permit any any <225.1.1.2/255.255.255.0>
switch(config-acl-ip)# 20 permit any any <239.1.1.2/255.255.255.0>
switch(config)-acl-ip# exit
switch(config)# router pim
switch(config-pim)# accept-rp <30.1.1.1> access-list <pim_rp_grp_acl>
switch(config-pim)# exit
switch(config)# access-list ip <pim_rpv6_grp_acl>
switch(config-acl-ipv6)# 10 permit any any <ff2e::2/64>
switch(config-acl-ipv6)# 20 permit any any <ff1e::1/64>
switch(config-acl-ipv6)# exit
switch(config)# router pim6
switch(config-pim6)# accept-rp <30::1> access-list <pim_rpv6_grp_acl>
switch(config-pim6)# exit

```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/multicast_5420-6200-6300-6400-8xxx-9300-10000/Content/Chp_pim-sm/pim-sm-ipv4_cmds/acc-rp.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	3.13 Deploy a Data Loss Prevention Solution Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			
v7	14.7 Enforce Access Control to Data through Automated Tools Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.			

3.3.1.3 PIM SSM (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

Protocol Independent Multicast - Source-Specific Multicast (PIM-SSM) is a specialized subset of PIM sparse mode that enables efficient delivery of multicast traffic from specific sources to receivers. It relies on IGMP version 3 (IGMPv3) for IPv4 and MLD version 2 (MLDv2) for IPv6 to allow receivers to explicitly specify the source from which they wish to receive multicast traffic. By default, PIM-SSM operates within the group range 232.0.0.0/8 for IPv4 and FF3x::/32 for IPv6. The feature also allows administrators to customize this range using an access list (ACL) to define valid multicast group addresses.

Rationale:

The design of PIM-SSM aligns with the goal of optimizing multicast traffic by allowing receivers to filter traffic based on source, thereby reducing overhead for both the network and end devices. The use of IGMPv3/MLDv2 protocols enables precise source selection, ensuring compatibility with modern network environments. The ability to modify the default SSM group range via ACLs provides network administrators with flexibility to tailor multicast configurations to meet specific organizational needs while adhering to operational constraints.

Impact:

PIM-SSM significantly improves multicast traffic efficiency by eliminating unnecessary traffic from unwanted sources, reducing network congestion, and ensuring only relevant multicast streams are delivered to receivers. However, modifying the PIM-SSM range can lead to temporary traffic loss as the system rebuilds multicast states, potentially disrupting application performance momentarily. Ensuring uniformity in the SSM range across a network is critical to maintaining seamless multicast traffic delivery and avoiding inconsistencies in routing behavior.

Audit:

To view the configuration change -

```
switch# show run pim
switch# show run pim6
```

Remediation:

Configuration to enable PIM-SSM Range ACL -

```

switch(config)# access-list ip <pim_ssm_grp_range_acl>
switch(config-acl-ip)# 10 permit any any <225.1.1.2/255.255.255.0>
switch(config-acl-ip)# 20 permit any any <239.1.1.2/255.255.255.0>
switch(config-acl-ip)# exit
switch(config)# router pim
switch(config-pim)# pim-ssm range-access-list <pim_ssm_grp_range_acl>
switch(config-pim)# exit
switch(config)# access-list ipv6 <pim_ssm_v6grp_range_acl>
switch(config-acl-ipv6)# 10 permit any any <ff2e::2/64>
switch(config-acl-ipv6)# 20 permit any any <ff1e::1/64>
switch(config-acl-ipv6)# exit
switch(config)# router pim6
switch(config-pim6)# pim-ssm range-access-list <pim_ssm_v6grp_range_acl>
switch(config-pim6)# exit

```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/multicast_5420-6200-6300-6400-8xxx-9300-10000/Content/Chp_pim-ssm/pim-ssm-ipv4_cmds/pim-ssm-rng-acc-list-v4.htm
2. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/multicast_5420-6200-6300-6400-8xxx-9300-10000/Content/Chp_pim-ssm/pim-ssm-ipv6_cmds/pim-ssm-rng-acc-list-v6.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	3.13 Deploy a Data Loss Prevention Solution Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			
v7	14.7 Enforce Access Control to Data through Automated Tools Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.			

3.3.2 SSDP (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

The Simple Service Discovery Protocol (SSDP) is an application layer protocol and one of the key protocols that implement Universal Plug and Play (UPnP). SSDP enables network devices to discover and advertise network services by sending multicast discovery and advertisement messages to multicast IPv4 group address 239.255.255.250:1900 or multicast IPv6 group address FF0x::C.

Rationale:

With UPnP, each device generates a unique multicast flow (Source IP, SSDP Group IP). In a multicast network with many end user devices, this can consume a large amount of multicast hardware and software resources as each device creates a unique (S, G) flow and the resources are limited.

Impact:

In networks where there is a need to control, drop, or minimize SSDP traffic, summarized static multicast routes can be configured to save network resources and to avoid denial of services.

Audit:

To view the configuration change -

```
switch# show ip multicast-static-route all-vrfs
```

Remediation:

The following example shows a typical static multicast route: [Incoming interface, Source, Group] > [Set of downstream interfaces] -

```
ip multicast-static-route <incoming-interface-name> {<source-address | any>}  
<group-address> [<outgoing-interface-name>] vrf <vrf-name>
```

If the SSDP service is not enabled in the network, best practices is to disable SSDP either through VLAN ACLs or through a policy, as shown in the following examples:

ACL -

```

switch(config)# access-list ip <drop_ssdp_acl>
switch(config-acl-ip)#10 deny udp any 239.255.255.250 eq 1900
switch(config)# vlan <id>
switch(config-vlan-id)# apply access-list ip <drop_ssdp_acl> in
switch(config)# interface <interface-id>
switch(config-if)# no shutdown
switch(config-if)# no routing
switch(config-if)# vlan access <id>
switch(config)# interface vlan <id>
switch(config-if-vlan)# ip address <ip-address>
switch(config-if-vlan)# ip igmp enable
switch(config-if-vlan)# ip pim-sparse enable
switch(config)# router pim
switch(config-pim)# enable

```

Policy -

```

switch(config)# class ip <drop_class>
switch(config-class-ip)# 10 match any any 239.255.255.250
switch(config)# policy <drop_ssdp_policy>
switch(config-policy)# 10 class ip <drop_class> action drop
switch(config)# vlan <id>
switch(config-vlan-id)# apply policy <drop_ssdp_policy> in
switch(config)# interface <interface-id>
switch(config-if)# no shutdown
switch(config-if)# no routing
switch(config-if)# vlan access <id>
switch(config)# interface vlan <id>
switch(config-if-vlan)# ip address <ip-address>
switch(config-if-vlan)# ip igmp enable
switch(config-if-vlan)# ip pim-sparse enable
switch(config)# router pim
switch(config-pim)# enable

```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/multicast_5420-6200-6300-6400-8xxx-9300-10000/Content/Chp_stat-rou/stat_rou_cmds/ip-mult-stat-rou.htm
2. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/multicast_5420-6200-6300-6400-8xxx-9300-10000/Content/Chp_stat-rou/use-case1.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.4 <u>Perform Traffic Filtering Between Network Segments</u> Perform traffic filtering between network segments, where appropriate.			
v7	14.2 <u>Enable Firewall Filtering Between VLANs</u> Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

3.3.3 IGMP Snooping ACL (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

IGMP snooping operates on a Layer 2 device as a multicast constraining mechanism designed to enhance multicast forwarding efficiency. It creates Layer 2 multicast forwarding entries by processing IGMP packets exchanged between hosts and routers. Without IGMP snooping, the switch would flood multicast packets to all hosts within a VLAN. By enabling IGMP snooping, the Layer 2 device forwards multicast packets associated with known multicast groups only to the receivers that have expressed interest, thereby conserving bandwidth on segments of the network where no hosts have requested the multicast traffic.

Rationale:

The device may encounter invalid multicast entries if malicious users send IGMP reports, which can disrupt multicast services for legitimate users. To address this, configuring a multicast group policy using an access control list (ACL) allows the Layer 2 device to control which multicast groups hosts can join. The device filters IGMP reports according to the policy and adds the host's port to the outgoing port list only if the report is permitted by the policy. This ensures that multicast traffic flows only to authorized groups, providing better security and optimized resource utilization.

Impact:

If an IGMPv3 packet contains multiple group addresses, the switch processes only the permitted group addresses per the ACL rules. Such packets are forwarded to the querier and PIM router, even if some group addresses are blocked. This prevents delays in learning permitted groups. If all group addresses in an IGMPv3 packet are denied by the ACL, the packet is not forwarded to the querier or PIM router, causing existing join messages for those groups to time out. For IGMPv2, if the packet does not match any rule or matches a deny rule, the packet is dropped, ensuring unauthorized multicast traffic is blocked.

Audit:

To view the configuration change -

```
switch# show run | in "ip igmp snooping"
```

Remediation:

To apply ACL to IGMP Snooping -

```
switch(config)# ip igmp snooping apply access list <ACL-NAME>
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/multicast_5420-6200-6300-6400-8xxx-9300-10000/Content/Chp_igmp_sno/igmp_sno_cmds/ip-igm-sno-acc-lis.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	3.13 <u>Deploy a Data Loss Prevention Solution</u> Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			
v7	14.7 <u>Enforce Access Control to Data through Automated Tools</u> Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.			

3.3.4 MLD Snooping ACL (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

Multicast Listener Discovery (MLD) snooping is a feature designed to optimize multicast traffic across the network by preventing multicast flooding within a VLAN. MLD snooping forwards multicast traffic only to ports that have initiated an MLD request for the multicast group. Additionally, MLD snooping supports configuration to drop packets that do not match the configured version and allows blocking multicast traffic on specific ports. This mechanism reduces unnecessary multicast traffic and improves network efficiency.

Rationale:

Similar to IGMP, malicious users can generate invalid multicast entries using MLD reports, which can overwhelm the device and disrupt legitimate multicast services. To mitigate this risk, a multicast group policy configured with an ACL is used to filter MLD reports. The Layer 2 device adds a host's port to the outgoing port list only if the MLD report complies with the policy. This ensures that only authorized multicast group traffic is forwarded, providing enhanced security and avoiding unnecessary resource consumption.

Impact:

When an ACL is applied to MLD snooping, only permitted group addresses in MLD packets are processed. The packets containing allowed group addresses are forwarded to the querier and PIM router, while the traffic for denied groups is blocked by the ACL. If all multicast groups in an MLD packet are denied by the ACL, the packet is not forwarded, and existing join messages for those groups will time out. Ports that do not match the MLD group policy are blocked from receiving multicast traffic, ensuring that unauthorized or excessive traffic does not propagate across the network.

Audit:

To view the configuration change -

```
switch# show run | in "ipv6 mld snooping"
```

Remediation:

To configure the MLD snooping ACL -

```
switch(config)# ipv6 mld snooping apply access list <ACL-NAME>
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/multicast_5420-6200-6300-6400-8xxx-9300-10000/Content/Chp_mlds/mlds_vlan_cfg_cmds/ipv6-mld-sno-app-acc-lis.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	3.13 <u>Deploy a Data Loss Prevention Solution</u> Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			
v7	14.7 <u>Enforce Access Control to Data through Automated Tools</u> Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.			

3.3.5 MSDP Authentication & SA Filtering (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

The Multicast Source Discovery Protocol (MSDP) connects multiple PIM-SM domains, enabling RPs to share multicast source information using SA messages over TCP. It simplifies interdomain multicast routing by supporting an interdomain source tree instead of a shared tree.

Rationale:

MSDP is crucial for efficient interdomain multicast routing in multi-domain networks. MD5 authentication secures peer connections, while ACL-based SA filtering allows precise traffic control, improving network performance and mitigating security risks.

Impact:

MSDP enhances multicast scalability by enabling cross-domain source discovery while reducing configuration complexity. Features like MD5 authentication and SA filtering improve security, optimize traffic flow, and prevent unauthorized or unnecessary data processing.

Audit:

To view the configuration change -

```
switch# show run msdp
```

Remediation:

Configuration to enable Authentication -

```
switch(config)# router msdp
switch(config-msdp)# ip msdp peer <ip-address>
switch(config-msdp-peer)# password plaintext <password>
```

User can prevent the incoming and outgoing SA messages on MSDP router by creating incoming and outgoing filter lists using an ACL.

Configuration to associate ACL -

```
switch(config-msdp-peer)# sa-filter in access-list <acl-name>
switch(config-msdp-peer)# sa-filter out access-list <acl-name>
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/multicast_5420-6200-6300-6400-8xxx-9300-10000/Content/Chp_msdp/mdsp_peer_cfg_cmds/sa-fil-acc-lis.htm
2. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/multicast_5420-6200-6300-6400-8xxx-9300-10000/Content/Chp_msdp/mdsp_peer_cfg_cmds/pas-msd.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

3.3.6 MSDP SA Cache limit (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

By default, the MSDP SA has no limit configured per peer. All (S, G) entries within the system capacities are allowed. If there is a reboot or HA switchover, the (S, G) cache allocation occurs based on first come first served basis. The (S, G) entries are allocated until they reach the system capacity or peer limit based on whichever is reached first and new sets of (S, G) requests are discarded.

Rationale:

The sa-limit command limits the overall number of (S, G) entries that a device can accept from specified MSDP peers and store in a SA-cache. When configured, the device maintains a per-peer count of (S, G) messages stored in the SA-cache and ignores new messages from a peer if the configured sa-limit for that peer has been reached. This command protects MSDP enabled devices from denial of service (DOS) attacks.

Impact:

Configuring the MSDP SA cache limit mitigates the risk of denial-of-service (DoS) attacks by restricting excessive multicast source entries. It prevents attackers from overwhelming the system with excessive SA messages, preserving network stability. Proper limits ensure resilience against DoS threats while maintaining reliable multicast traffic handling.

Audit:

To view the configuration change -

```
switch# show run msdp
```

Remediation:

Configuration to enable MSDP SA cached limit -

```
switch(config)#router msdp
switch(config-msdp)#ip msdp peer <peer-address>
switch(config-msdp)#sa-limit <value>
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/multicast_5420-6200-6300-6400-8xxx-9300-10000/Content/Chp_msdp/msdp_rou_cfg_cmds/sa-lim.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</u> Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.			
v8	<u>7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets</u> Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.			
v8	<u>13.5 Manage Access Control for Remote Assets</u> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v7	<u>12.2 Scan for Unauthorized Connections across Trusted Network Boundaries</u> Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.			

3.3.7 Multicast Boundary ACL (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

A multicast boundary ACL (Access Control List) is a configuration mechanism that filters multicast traffic at specified interfaces to control the routing of multicast packets. This feature works on Point-to-Point links, including ROP/L3 LAG or Point-to-Point SVI, and can manage both multicast data and control packets, such as IGMP joins and PIM join/prune messages. The ACL rules can match multicast group entries (*,G) and use subnet masks to define address ranges, supporting IP, IGMP, and PIM protocols. While MSDP (Multicast Source Discovery Protocol) continues to forward source announcements (SA messages) across boundaries regardless of ACL configurations, multicast boundary ACLs play a crucial role in defining which multicast traffic is permitted or denied between different domains. The feature is IPv4-specific and does not support Anycast RP with MSDP mesh groups across boundaries. For filtering PIM bootstrap messages, a separate pim bsr-boundary configuration is required

Rationale:

The primary rationale for implementing multicast boundary ACLs is to enforce traffic control and domain isolation in multicast-enabled networks. By filtering multicast traffic at the interface level, organizations can prevent unwanted or unauthorized multicast traffic from being routed across domains, which helps maintain network security and stability. The ability to match specific group addresses, such as the example where traffic for 239.0.0.0/8 is denied while 224.0.0.0/4 is permitted, gives network administrators granular control over traffic policies. This control is critical in preventing multicast routing loops, managing traffic congestion, and ensuring that only necessary multicast traffic flows between domains.

Impact:

Configuring multicast boundary ACLs has a significant impact on network performance, security, and traffic management. By applying filters in both inbound and outbound directions, the feature ensures that only authorized multicast traffic crosses domain boundaries, reducing the likelihood of network overload or disruptions caused by excessive or misrouted multicast packets. It also enhances security by isolating multicast domains, preventing unauthorized traffic from infiltrating sensitive areas of the network.

Audit:

To view the configuration change -

```
switch# show run
```

Remediation:

The boundary ACL example shown below creates a boundary where group address in 239.0.0.0/8 is denied and all other group addresses in 224.0.0.0/4 are permitted. Since the source address is any, it matches (*,G) traffic. The boundary will be applied in both in and outbound directions.

```
access-list ip bound
 10 deny any any 239.0.0.0/255.0.0.0
 20 permit any any 224.0.0.0/240.0.0.0
interface lag 1
 ip address 40.1.1.1/24
 ip pim-sparse enable
 ip multicast boundary access-list bound
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/multicast_5420-6200-6300-6400-8xxx-9300-10000/Content/Chp_pim-sm/pim-ip-mcst/ip-mcst-bnd.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

3.3.8 Multicast BSR Boundary (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

PIM Bootstrap messages (BSMs) play a crucial role in electing a Rendezvous Point (RP) for multicast routing within a domain. However, exchanging these messages across different multicast domains is undesirable, as it can result in the unintended election of an RP in a domain where it does not belong, disrupting multicast operations. To address this, the bsr-boundary configuration can be applied to boundary interfaces, ensuring that PIM BSMs originating from external domains are dropped and that internally generated BSMs are confined to their domain.

Rationale:

The rationale for restricting the propagation of PIM Bootstrap messages across multicast boundaries is to preserve the integrity and isolation of domain-specific RP elections. Allowing such messages to traverse domains can lead to conflicts or misconfigurations, where RPs are incorrectly elected in domains they are not supposed to serve. By using the bsr-boundary feature, network administrators can enforce strict boundaries, ensuring that multicast routing remains consistent and domain-specific, preventing cross-domain interference.

Impact:

Implementing the bsr-boundary configuration has a significant impact on maintaining the stability and efficiency of multicast routing. It prevents RP election conflicts across domains, ensuring that each multicast domain operates independently and without disruption.

Audit:

To view the configuration change in the interface -

```
switch# show run interface
```

Remediation:

Configuration to enable Multicast BSR Boundary -

```
switch(config)# interface <ID>
switch(config-int)# ip pim-sparse bsr-boundary
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/multicast_5420-6200-6300-6400-8xxx-9300-10000/Content/Chp_pim-sm/pim-sm-ipv4_cmds/ip-pim-spa-bsr.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	12.4 Deny Communication over Unauthorized Ports Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.			

3.4 IP Source Lockdown (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

IP source lockdown provides added security by preventing IP source address spoofing on a per-port basis. Every packet is inspected for this purpose in hardware. When IP source lockdown is enabled, IP traffic received on an interface (port) is forwarded only if the VLAN, IP address, MAC address, and interface (port) match the IP binding database entry. To use IP source lockdown, the IP binding database must be populated. The binding database is dynamically populated by DHCP snooping that learns and saves the binding information. Alternatively, the IP binding database can be statically populated with the `ip source-binding` command.

Rationale:

The IP Source Lockdown feature on AOS-CX switches enhances network security by preventing unauthorized devices from spoofing IP addresses. It ensures that only legitimate devices with pre-approved IP-to-MAC bindings can communicate on the network. This minimizes risks of IP spoofing attacks and unauthorized access.

Impact:

By implementing IP Source Lockdown, organizations can significantly reduce vulnerabilities to man-in-the-middle attacks, unauthorized device access, and network disruptions. This improves overall network integrity, enhances compliance with security policies, and ensures reliable and secure connectivity for critical business operations.

Audit:

To view the IPv4 source lockdown information -

```
show ipv4 source-lockdown [binding [interface <IFNAME> | ip <IPV4-ADDR> | mac <MAC-ADDR> | vlan <VLAN-ID>] | interface <IFNAME>]
```

Following command shows all IPv4 static source binding information irrespective of source lockdown configuration -

```
show ipv4 source-binding
```

To view the IPv6 source lockdown information -

```
show ipv6 source-lockdown [binding [interface <IFNAME> | ip <IPV6-ADDR> | mac <MAC-ADDR> | vlan <VLAN-ID>] | interface <IFNAME>]
```

Following command shows all IPv6 static source binding information irrespective of source lockdown configuration -

```
show ipv6 source-binding
```

Remediation:

To enable IP source lockdown resource extended on the device (supports dynamically sharing hardware resources of IP source lockdown with other features) -

```
switch(config)# ip source-lockdown resource-extended
```

To enable IPv4/IPv6 source lockdown for all VLANs on the selected interface (port) -

```
switch(config)# interface <interface-id>  
switch(config-if)# ipv4 source-lockdown  
switch(config-if)# ipv6 source-lockdown
```

To add static IPv4/IPv6 client source binding information to the switch IPv4/IPv6 binding database -

```
Ipv4 source-binding <VLAN-ID> <IPV4-ADDR> <MAC-ADDR> <IFNAME>  
ipv6 source-binding <VLAN-ID> <IPV6-ADDR> <MAC-ADDR> <IFNAME>
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/ip_services_6300-6400/Content/Chp_IP_sou_LD/ip-sou-loc-630-840-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.12 Segment Data Processing and Storage Based on Sensitivity Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.			
v7	14.1 Segment the Network Based on Sensitivity Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).			

3.5 Dynamic ARP Inspection (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

Dynamic ARP Inspection (DAI) is a security feature available in AOS-CX switches that validates ARP packets on the network to prevent ARP spoofing and ARP-based man-in-the-middle attacks. It verifies ARP requests and responses against trusted sources, such as DHCP snooping and static ARP entries.

Rationale:

Dynamic ARP inspection ensures that ARP traffic is authenticated before being forwarded, preventing attackers from injecting forged ARP packets to redirect traffic. This feature is critical in maintaining the integrity of Layer 2 networks and protecting devices from malicious attempts to hijack IP addresses.

Impact:

Implementing Dynamic ARP Inspection enhances network security by blocking malicious ARP packets and mitigating risks of ARP-based attacks. It reduces downtime caused by compromised devices and ensures reliable communication in enterprise environments. However, misconfiguration or lack of trusted entries may disrupt legitimate traffic.

Audit:

To View the ARP Inspection configuration & Statistics -

```
switch# show arp inspection [interface | vlan]
switch# show arp inspection statistics
```

Remediation:

Following command enables Dynamic ARP inspection on the current VLAN, which means that ARP packets received from untrusted interfaces are discarded if they have an Invalid IP-to-MAC address binding -

```
switch(config)# vlan <vlan-id>
switch(config-vlan)# arp inspection
```

Configures the interface as a trusted. All interfaces are untrusted by default -

```
switch(config)# interface <interface-id>
switch(config-if)# arp inspection trust
```

Dynamic ARP Inspection is enforced using DHCP Snooping binding and Static IP Binding. Refer to the DHCP Snooping section for the DHCP snooping configuration. To enable the Static IP Binding use the below configuration -

```
switch(config)# vlan <vlan-id>
switch(config-vlan)# arp ipv4 <IPV4_ADDR> mac <MAC_ADDR>
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/ip_services_6300-6400/Content/Chp_ARP/ARP_cmds/arp-ins-fl-xl-ml-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	12.4 Deny Communication over Unauthorized Ports Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.			

3.6 ND Snooping (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

ND (Neighbor Discovery) Snooping is a security feature that enhances IPv6 network integrity by monitoring and validating IPv6 neighbor discovery messages. It prevents malicious activities such as ND spoofing and rogue advertisements. ND snooping drops invalid ND packets, and combined with IPv6 Source Lockdown, blocks data traffic from invalid hosts. ND snooping learns the source MAC addresses, source IPv6 addresses, input interfaces and VLANs of incoming ND messages and data packets to build IP binding entries. ND snooping drops ND packets for the following reasons:

- If the Ethernet source MAC address does not match the address in the ICMPv6 Target link layer address field of the ND packet.
- If the global IPv6 address in the source address field does not match the ND snooping prefix filter table.
- If the global IPv6 address or the link-local IPv6 address in the source IP address field does not match

the ND snooping binding table.

Rationale:

The feature ensures that only legitimate IPv6 devices can communicate on the network by maintaining a trusted ND cache. This reduces vulnerabilities and strengthens Layer 2 and Layer 3 IPv6 communication.

Impact:

ND Snooping improves network security by mitigating IPv6-based attacks, enhances device discovery accuracy, and ensures reliable communication between endpoints in IPv6 environments.

Audit:

To view the ND snooping configuration -

```
switch # show nd-snooping
```

Remediation:

The following are sample VLAN configurations of globally enabled ND snooping -

```
switch(config)# nd-snooping
switch(config)# vlan <vlan-id>
switch(config-vlan-id)# nd-snooping
switch(config-vlan-id)# exit
switch(config)#
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/ip_services_6300-6400/Content/Chp_NDsnoop/nd-sno-630-10.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.12 Segment Data Processing and Storage Based on Sensitivity Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.			
v7	14.1 Segment the Network Based on Sensitivity Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).			

3.7 RA Guard (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

RA (Router Advertisement) Guard is a security feature in AOS-CX switches that monitors and filters IPv6 Router Advertisement messages, allowing only authorized RAs to propagate. It helps prevent rogue or malicious routers from disrupting network operations. When RA guard policy is enabled (with ipv6 nd-snooping ra-guard policy), RA packets received on trusted ports are validated against a set of parameters configured on the policy and assigned to a port or VLAN. RA Guard policy options include:

- Hop Limit
- Managed Config Flag
- Other Config Flag
- Router Preference
- ACL
- Advertised Prefix Lists

Rationale:

The feature ensures that only trusted router advertisements can influence the IPv6 routing environment. This is critical for maintaining the integrity of the routing configuration and mitigating attacks like rogue RA injection and man-in-the-middle exploits.

Impact:

By deploying RA Guard, network administrators can prevent unauthorized devices from acting as routers, reducing the risk of network disruptions and enhancing overall IPv6 network stability, security, and performance.

Audit:

To view the RA guard configuration -

```
switch# show nd-snooping ra-guard interface <interface-id>
```

Remediation:

This command enables Routing Advertisement (RA) guard on the selected VLAN. When enabled, ingress Routing Advertisement (RA) packets on the selected VLAN are blocked on untrusted ports. The packets are forwarded when received on trusted ports -

```
switch(config)# nd-snooping enable
switch(config)# vlan <id>
switch(config-vlan-id)# nd-snooping ra-guard
switch(config-vlan-id)# exit
switch(config)#
```

Following commands enables RA guard policy, hence RA packets received on trusted ports are validated against a set of parameters configured on the policy and assigned to a port or VLAN -

```
switch(config)# ipv6 nd-snooping ra-guard policy <POLICY-NAME>
switch(config-raguard-policy)# hop-limit <enable | minimum | maximum>
switch(config-raguard-policy)# match <access-list | prefix-list>
switch(config-raguard-policy)# managed-config-flag <on | off>
switch(config-raguard-policy)# other-config-flag <on | off>
switch(config-raguard-policy)# router-preference <high | medium | low>
switch(config-raguard-policy)# exit
switch(config)# vlan <id>
switch(config-vlan-id)# nd-snooping ra-guard attach-policy POLICY_NAME
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/ip_services_6300-6400/Content/Chp_NDsnoop/NDsnoop_cmds/nd-sno-ra-gua-ml-xl-10.htm
2. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/ip_services_6300-6400/Content/Chp_NDsnoop/RAguard_pol_cmds/nd-sno-ra-gua-pol.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	3.12 <u>Segment Data Processing and Storage Based on Sensitivity</u> Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.			
v8	3.13 <u>Deploy a Data Loss Prevention Solution</u> Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			
v8	13.4 <u>Perform Traffic Filtering Between Network Segments</u> Perform traffic filtering between network segments, where appropriate.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	14.1 <u>Segment the Network Based on Sensitivity</u> Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).			
v7	14.2 <u>Enable Firewall Filtering Between VLANs</u> Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			
v7	14.7 <u>Enforce Access Control to Data through Automated Tools</u> Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.			

3.8 IPv6 Destination Guard (Manual)

Profile Applicability:

- Optional Security Recommendations

Description:

The IPv6 Destination Guard feature in AOS-CX switches provides security by validating IPv6 traffic against a known database of allowed destinations. It ensures only authorized destination IP addresses are reachable, mitigating risks of unauthorized access or malicious activity within the network. This feature requires the binding table to be populated with the help of DHCPv6 snooping, ND snooping, or static-ip-bindings. Destination guard enables the destination address based filtering of IPv6 traffic and blocks the Neighbor Discovery (ND) protocol resolution for destination addresses that are not found in the binding table.

Rationale:

With the growing adoption of IPv6, networks are exposed to a wider attack surface. IPv6 Destination Guard helps secure the network by filtering traffic based on trusted destination addresses, preventing spoofing or unauthorized communication to sensitive resources.

Impact:

Implementing IPv6 Destination Guard enhances network security by mitigating threats like IPv6 address spoofing and unauthorized data exfiltration. It contributes to a robust, reliable, and secure network environment by ensuring only legitimate IPv6 destinations are accessible.

Audit:

This command displays ipv6 destination-guard configuration -

```
switch# show ipv6 destination-guard
```

Remediation:

Configuring IPV6 Destination Guard on a VLAN -

```
switch(config)# vlan <id>  
switch(config-vlan-<id>)# ipv6 destination-guard
```

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/ip_services_6300-6400/Content/Chp_Dest_guard/Dest_guard_cmds/ipv6-des-gua.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.13 <u>Deploy a Data Loss Prevention Solution</u> Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			●
v8	7.5 <u>Perform Automated Vulnerability Scans of Internal Enterprise Assets</u> Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	7.6 <u>Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets</u> Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		●	●
v8	13.5 <u>Manage Access Control for Remote Assets</u> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.		●	●
v7	12.2 <u>Scan for Unauthorized Connections across Trusted Network Boundaries</u> Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.		●	●
v7	13.3 <u>Monitor and Block Unauthorized Network Traffic</u> Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

4 Control Plane

The switch control plane is responsible for making decisions about how network traffic should be handled and routed, determining the best paths for data to travel through the network. Traffic information from the data plane is sent to the control plane, where the CPU determines how the information is handled. Controlling the type and amount of information forwarded to the CPU is critical to maintaining efficient operation of the switch.

4.1 COPP Policing

Control Plane Policing (CoPP) is a security feature that protects a router's control plane CPU from data plane denial-of-service (DoS) attacks. By rate-limiting or dropping specific types of traffic from the data plane to the CPU, CoPP ensures the CPU remains available to handle essential network operations, such as routing updates and management traffic. In a well-planned CoPP policy, network traffic is classified based on the type of traffic, which can be management traffic, routing protocols, or known IP addresses.

4.1.1 Control Plane Policing (Manual)

Profile Applicability:

- Level 2

Description:

This sequence describes configuring Control plane policing (CoPP)

Rationale:

Control Plane Policing prevents flooding of certain types of packets from overloading the switch or module CPU by either rate-limiting or dropping packets.

The switch software provides several configurable classes of packets that can be rate-limited, including (but not limited to) ARP broadcasts, multicast, routing protocols (BGP, OSPF), and spanning tree. CoPP is always active and cannot be disabled.

Impact:

CoPP is crucial for protecting the control plane and preventing network outages. It does, however, require careful configuration and monitoring to avoid unintended side effects. Misconfiguration can lead to performance degradation, network disruptions, and management issues, such as:

- **Excessive Policing:** Overly restrictive CoPP policies can drop legitimate control plane traffic, leading to delayed or lost routing updates, impaired management access, and potentially impacting network performance.
- **CPU Cycle Consumption:** If not configured effectively it can consume CPU cycles.
- **Slow or Unresponsive CLI Sessions:** High CPU utilization or resource exhaustion caused by excessive traffic to the control plane can make interactive sessions via the command-line interface (CLI) slow or unresponsive.
- **Route Flaps:** Excessive policing of line protocol keepalives or routing protocol updates (like BGP or OSPF updates) can lead to unstable routing, route flaps, neighbor adjacency flaps or timeouts, causing network instability.
- **Resource Exhaustion:** A poorly configured CoPP policy could lead to route processor resource exhaustion, resulting in resources like memory and buffers becoming unavailable for legitimate IP data packets.
- **Unintended Errors:** Incorrectly configured CoPP policies can lead to unintended consequences, such as blocking legitimate traffic or failing to adequately protect the control plane.

Audit:

Syntax:

```
switch# show copp-policy <policy_name>
```

Example 1:

```
switch# show copp-policy test_1
class          drop priority rate pps burst pkts hardware rate pps
-----
acl-logging    1          50    100    50
default        2        4225    528   4225
switch#
```

Example 2:

```
switch# show copp-policy default
copp-policy default
  class acl-logging priority 0 rate 25 burst 25
  class arp-broadcast priority 2 rate 1250 burst 1250
  class arp-protect priority 2 rate 2075 burst 2075
  class arp-unicast priority 3 rate 825 burst 825
  class bfd-control priority 5 rate 850 burst 850
  class bgp priority 5 rate 1025 burst 750
  class captive-portal priority 2 rate 2075 burst 259
  class client-onboard priority 5 rate 1024 burst 1024
  class dfp-collector priority 0 rate 512 burst 512
  class dhcp priority 2 rate 750 burst 750
  class erps priority 6 rate 225 burst 225
  class fib-optimization priority 0 rate 100 burst 200
  class icmp-broadcast-ipv4 priority 2 rate 325 burst 325
  class icmp-multicast-ipv6 priority 2 rate 475 burst 475
  class icmp-security-ipv6 priority 2 rate 325 burst 325
  class icmp-unicast-ipv4 priority 3 rate 225 burst 225
  class icmp-unicast-ipv6 priority 3 rate 400 burst 400
  class ieee-8021x priority 2 rate 2075 burst 259
  class igmp priority 4 rate 1600 burst 450
  class ip-exceptions priority 0 rate 100 burst 100
  class ip-lockdown priority 0 rate 100 burst 100
  class ip-tracker priority 0 rate 256 burst 256
  class ipfix priority 0 rate 2500 burst 2500
  class ipsec priority 5 rate 1025 burst 128
  class ipv4-options priority 1 rate 100 burst 100
  class lacp priority 5 rate 2050 burst 2050
  class lldp priority 5 rate 100 burst 100
  class loop-protect priority 6 rate 225 burst 225
  class mac-lockout priority 0 rate 100 burst 100
  class manageability priority 4 rate 4218 burst 4218
  class mdns priority 2 rate 150 burst 150
  class mirror-to-cpu priority 0 rate 100 burst 100
  class mld priority 4 rate 1600 burst 450
  class mvrp priority 5 rate 425 burst 225
  class nae-packet-monitor priority 0 rate 100 burst 200
  class ntp priority 4 rate 100 burst 100
  class ospf-multicast priority 5 rate 1025 burst 1025
  class ospf-unicast priority 5 rate 1025 burst 1025
  class pim priority 5 rate 1700 burst 1700
  class ptp priority 5 rate 1000 burst 250
  class secure-learn priority 2 rate 2075 burst 259
  class sflow priority 1 rate 1000 burst 125
  class stp priority 6 rate 2000 burst 2000
  class udld priority 6 rate 450 burst 450
  class unknown-multicast priority 1 rate 1025 burst 128
  class unresolved-ip-unicast priority 1 rate 325 burst 325
  class vrrp priority 4 rate 400 burst 400
  default-class priority 2 rate 4225 burst 528
apply copp-policy default
switch#
```

Remediation:

Syntax:

```

switch# config
switch(config)# copp-policy test_1
switch(config-copp)# class <class> ?
    drop                Drop packets matching this class
    factory-default     Set this class to factory default configuration
    priority            Specify the priority for this class

switch(config-copp)# class <class> drop ?

switch(config-copp)# class <class> factory-default ?

switch(config-copp)# class <class> priority ?
    <0-6>               The priority for this class
switch(config-copp)# class <class> priority <0-6> ?
    rate               Specify the rate for this class
switch(config-copp)# class <class> priority <priority> rate ?
    <25-99999>         The rate for this class in units of packets per second
switch(config-copp)# class <class> priority <priority> rate <rate> ?
    burst              Specify the burst for this class
    <cr>
switch(config-copp)# class <class> priority <priority> rate <rate> burst ?
    <1-9999>           The burst for this class in units of packets
switch(config-copp)# class <class> priority <0-6> rate <25-99999> burst <1-9999> ?
<cr>
switch(config-copp)# exit
switch(config)#

```

Example:

```

6300# config
6300(config-copp)# copp-policy test_1
6300(config-copp)# class acl-logging priority 1 rate 50 burst 100
6300(config-copp)# default-class priority 2 rate 4225 burst 528
6300(config-copp)# exit
6300(config)# exit
6300#

```

Default Value:

```

switch# show copp-policy factory-default
class                drop priority rate pps burst pkts hardware rate pps
-----
acl-logging          0          25      25      25
arp-broadcast         2        1250    1250    1250
arp-protect           2        2075    2075    2075
arp-unicast           3         825     825     825
bfd-control           5         850     850     850
bgp                   5        1025    750     1025
captive-portal        2        2075    259     2075
client-onboard        5        1024    1024    1000
dfp-collector         0         512     512     500
dhcp                  2         750     750     750
erps                  6         225     225     225
fib-optimization      0         100     200     100
icmp-broadcast-ipv4   2         325     325     325
icmp-multicast-ipv6   2         475     475     475
icmp-security-ipv6    2         325     325     325
icmp-unicast-ipv4     3         225     225     225
icmp-unicast-ipv6     3         400     400     400
ieee-8021x            2        2075    259     2075
igmp                  4        1600    450     1600
ip-exceptions         0         100     100     100
ip-lockdown           0         100     100     100
ip-tracker            0         256     256     250
ipfix                 0        2500    2500    2500
ipsec                 5        1025    128     1025
ipv4-options          1         100     100     100
lacp                  5        2050    2050    2050
lldp                  5         100     100     100
loop-protect          6         225     225     225
mac-lockout           0         100     100     100
manageability         4        4218    4218    4200
mdns                  2         150     150     150
mirror-to-cpu         0         100     100     100
mld                   4        1600    450     1600
mvrp                  5         425     225     425
nae-packet-monitor    0         100     200     0
ntp                   4         100     100     100
ospf-multicast        5        1025    1025    1025
ospf-unicast          5        1025    1025    1025
pim                   5        1700    1700    1700
ptp                   5        1000    250     1000
secure-learn          2        2075    259     2075
sflow                 1        1000    125     1000
stp                   6        2000    2000    2000

```

udld	6	450	450	450
unknown-multicast	1	1025	128	1025
unresolved-ip-unicast	1	325	325	325
vrrp	4	400	400	400
default	2	4225	528	4225
switch#				

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/hardening/Content/Chp_hard-ctrl/ctrl-pln-polic.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.13 <u>Deploy a Data Loss Prevention Solution</u> Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			●
v7	13.3 <u>Monitor and Block Unauthorized Network Traffic</u> Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

4.2 Spanning Tree Security

Spanning Tree Protocol (STP) helps secure a network by preventing network loops, which can lead to broadcast storms and network instability. Broadcast storms occur when broadcast packets circulate endlessly through redundant paths, consuming bandwidth and potentially crashing network devices

4.2.1 Spanning Tree BPDU Protect (Manual)

Profile Applicability:

- Level 1

Description:

This sequence describes configuring Spanning Tree's BPDU Protect feature

Rationale:

Various security mechanisms are in place to protect spanning tree configurations from interference and rogue devices or unwarranted changes to the network. BPDU protection secures the active topology by preventing spoofed BPDU packets from entering the network. Typically, BPDU protection is applied on edge ports connected to end user devices that do not run STP. If STP BPDU packets are received on a protected port, BPDU guard disables the port and an alert is sent.

Impact:

While BPDU protect will prevent spoofed BPDU traffic from entering the network, there are potential impacts to the network including: When a BPDU packet is received the receiving port enters an error state and shuts down, resulting in loss of connectivity of connected devices. If BPDU protect is mis-configured and enabled on a port connected to another switch actively participating in the spanning tree, a loop can occur, leading to broadcast storms and network instability.

Audit:

Audit Procedure

```

switch# show spanning-tree interface 1/1/20
Port                               : 1/1/20
Admin State                        : up
BPDU Guard                        : enabled
BPDU Filter                       : disabled
RPVST Guard                       : disabled
RPVST Filter                      : disabled
Loop Guard                        : disabled
Root Guard                        : disabled
TCN Guard                         : disabled
Admin Edge Port                   : admin-network
Link Type                         : Point to Point
BPDU Tx Count                     : 31
BPDU Rx Count                     : 0
TCN Tx Count                      : 0
TCN Rx Count                      : 0

```

Remediation:

```

switch(config)# interface 1/1/20
switch(config-if)# no shutdown
switch(config-if)# no routing
switch(config-if)# vlan access 10
switch(config-if)# spanning-tree bpdu-guard
switch(config-if)# exit

```

Default Value:

Spanning Tree BPDU protect is disabled by default

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/hardening/Content/Chp_hard-ctrl/sec-span-tree.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.			
v8	7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.			

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.5 <u>Manage Access Control for Remote Assets</u> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v7	12.2 <u>Scan for Unauthorized Connections across Trusted Network Boundaries</u> Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.			

4.2.2 Spanning Tree Root Protect (Manual)

Profile Applicability:

- Level 1

Description:

This sequence describes configuring Spanning Tree's Root Protect feature

Rationale:

Root protection secures the active topology by preventing other switches from declaring their ability to propagate superior BPDUs, containing both better information on the root bridge and path cost to the root bridge which would normally replace the current root bridge selection. This is typically carried out between the core that is required to be the root and access switches to prevent ports that are not expected to originate root information such as server ports and access switch ports.

Impact:

Enabling the Spanning Tree Protocol (STP) Root Guard feature, also known as Root Protect, is a crucial security measure in network switches. It helps prevent unauthorized switches from becoming the root bridge in your network's STP topology. However, like any network configuration, there can be potential side effects if not implemented correctly:

Ports in Root-Inconsistent State: If a port receives a superior Bridge Protocol Data Unit (BPDU) the port enters a "root-inconsistent" state and stops forwarding traffic.

Potential for Unexpected Topology Changes: If Root Guard is erroneously enabled on ports that are supposed to be part of the root path, it could block legitimate switches from becoming the root bridge in case of a failure, which could lead to network instability. Root Guards implementation can influence how the spanning tree converges. Incorrectly chosen root bridges can lead to suboptimal paths for data traffic, potentially impacting network performance.

Audit:

```
switch# show spanning-tree interface 1/1/21
Port                               : 1/1/21
Admin State                        : up
BPDU Guard                        : disabled
BPDU Filter                       : disabled
RPVST Guard                       : disabled
RPVST Filter                      : disabled
Loop Guard                       : disabled
Root Guard                        : enabled
TCN Guard                        : disabled
Admin Edge Port                   : admin-network
Link Type                         : Point to Point
BPDU Tx Count                     : 31
BPDU Rx Count                     : 0
TCN Tx Count                      : 0
TCN Rx Count                      : 0
```

Remediation:

```
switch(config)# interface 1/1/21
switch(config-if)# no shutdown
switch(config-if)# no routing
switch(config-if)# vlan trunk allow all
switch(config-if)# vlan trunk native 1
switch(config-if)# spanning-tree root-guard
switch(config-if)# exit
```

Default Value:

Spanning Tree root protect is disabled by default

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/hardening/Content/Chp_hard-ctrl/sec-span-tree.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

4.3 Control Plane ACL

Once an IP address is bound to an interface associated with a VRF, the switch may become exposed to management access from untrusted users or devices. This potential point of vulnerability can be mitigated by binding an Access Control List (ACL) to the control plane for that VRF. The control plane handles the device's management and routing functionality. Once a control plane ACL is applied to a VRF, it filters packets to all IPv4/IPv6 addresses bound to the device on that VRF. It is possible to create a control plane ACL for each existing VRF, including the mgmt VRF.

4.3.1 Control Plane ACL Management (Manual)

Profile Applicability:

- Level 2

Description:

Restrict Management Access to trusted management devices

Rationale:

Restricting what devices are allowed to access your network infrastructure helps reduce credential stuffing and man-in-the-middle (MITM) attacks.

Impact:

There are significant risks associated with allowing any device with reachability to access the exposed ports on network infrastructure. White listing specific devices to allow specific interfaces ensures only specific devices will be able to access specific interfaces.

Audit:

```
switch# show access-list control-plane
```

Remediation:

```
switch# conf
switch(config)# access-list ip <acl-name>
switch(config-acl-ip)# permit ip <ip address or network> any
switch(config-acl-ip)# deny ip any any log
switch(config)# apply access-list ip <acl-name> control-plane vrf mgmt
```

Default Value:

No ACL is applied by default

References:

1. https://arubanetworking.hpe.com/techdocs/AOS-CX/10.15/HTML/hardening/Content/Chp_hard-mgmt/ctrl-plane-acl.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	3.13 <u>Deploy a Data Loss Prevention Solution</u> Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			
v7	14.7 <u>Enforce Access Control to Data through Automated Tools</u> Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.			

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	Management		
1.1	Securing Switch Management Access		
1.1.1	Create security user group (Manual)	☐	☐
1.1.2	Securing Password Entry (Manual)	☐	☐
1.1.3	Hardening Password Rules (Automated)	☐	☐
1.1.4	Set an Export Password (Automated)	☐	☐
1.1.5	Enable Enhanced Secure Mode (Manual)	☐	☐
1.1.6	Default admin account password (Manual)	☐	☐
1.1.7	RBAC - Customer defined local user groups (Manual)	☐	☐
1.1.8	Session Management (Automated)	☐	☐
1.1.9	Verifying Telnet Server is Disabled (Automated)	☐	☐
1.1.10	Using Local RBAC to Limit User Access to Shell (Manual)	☐	☐
1.2	Securing SSH		
1.2.1	SSH Public Key Authentication (Automated)	☐	☐
1.2.2	SSH Allow List (Automated)	☐	☐
1.2.3	SSH Server Port Customization (Automated)	☐	☐
1.2.4	Recommended Ciphers, MACs, and Algorithms (Manual)	☐	☐
1.2.5	Two-factor authentication with the SSH server (Automated)	☐	☐
1.2.6	SSH Server Key (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.3	Securing Time Synchronization		
1.3.1	NTP Authentication (Automated)	☐	☐
1.3.2	Configuring Time Services (Automated)	☐	☐
1.4	Securing SNMP Access		
1.4.1	SNMP Community		
1.4.1.1	Non Default Community Names, Access Rights & ACL (Automated)	☐	☐
1.4.2	SNMPv3 Enablement		
1.4.2.1	SNMP V3 (Automated)	☐	☐
1.4.3	SNMP Traps (Automated)	☐	☐
1.5	AAA for Management Interfaces		
1.5.1	Remote AAA Servers		
1.5.1.1	Radius Server Configuration (Automated)	☐	☐
1.5.1.2	TACACS Server Configuration (Automated)	☐	☐
1.5.1.3	RadSec Server Configuration (Manual)	☐	☐
1.5.2	Authentication		
1.5.2.1	Default & Fallback Local Authentication (Manual)	☐	☐
1.5.2.2	Limit Login Attempts (Automated)	☐	☐
1.5.2.3	Remote Authentication - RADIUS/RadSec/TACACS+ (Automated)	☐	☐
1.5.3	Authorization		
1.5.3.1	Local Authorization (Automated)	☐	☐
1.5.3.2	Remote Authorization (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.5.4	Accounting		
1.5.4.1	Local Accounting (Automated)	☐	☐
1.5.4.2	Remote Accounting (Automated)	☐	☐
1.5.5	Per User Management Interface Enablement (Manual)	☐	☐
1.5.6	Login Privilege Elevation for Administrators (Automated)	☐	☐
1.6	Public Key Infrastructure (PKI)		
1.6.1	TLS Check Key Usage (Manual)	☐	☐
1.6.2	TLS Minimum Version (Automated)	☐	☐
1.7	Firmware		
1.7.1	Firmware Validation (Manual)	☐	☐
1.8	Securing File Transfer		
1.8.1	SCP and SFTP		
1.8.1.1	SFTP and SCP (Manual)	☐	☐
1.9	Securing the https-server		
1.9.1	https-server default enablement (Automated)	☐	☐
1.9.2	https-server idle session management (Automated)	☐	☐
1.9.3	Two-factor authentication with the https-server server (Automated)	☐	☐
1.9.4	Assign a custom certificate to the https-server (Manual)	☐	☐
1.10	Enable ServiceOS Password Authentication		
1.10.1	ServiceOS Password (Automated)	☐	☐
1.11	Securing Syslog		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.11.1	Assign a custom certificate to syslog-client (Manual)	☐	☐
1.11.2	Configure syslog-client to log using TLS (Automated)	☐	☐
1.12	Login Banner (Automated)	☐	☐
1.13	Schedule Configuration Backup Job (Automated)	☐	☐
1.14	Create Hostname (Automated)	☐	☐
2	Interface		
2.1	Physical Security		
2.1.1	Disable USB and Bluetooth on Device (Automated)	☐	☐
2.1.2	Front Panel Security (Manual)	☐	☐
2.1.3	Disable Unused Physical Interfaces (Manual)	☐	☐
2.2	Traffic Control - Rate limiting (Manual)	☐	☐
2.3	Proxy ARP (Manual)	☐	☐
2.4	IP Directed Broadcast (Manual)	☐	☐
3	Protocol		
3.1	Routing Protocols		
3.1.1	OSPF		
3.1.1.1	OSPF Passive Interfaces (Manual)	☐	☐
3.1.1.2	OSPF Neighbor Authentication (Manual)	☐	☐
3.1.1.3	OSPFv3 Area Authentication and Encryption with IPsec (Manual)	☐	☐
3.1.2	BGP		
3.1.2.1	Control Plane ACL for BGP Peering Sessions (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.1.2.2	Authenticate BGP Peers Using MD5 (Manual)	☐	☐
3.1.2.3	BGP TTL Security (Manual)	☐	☐
3.2	DHCP Protocols		
3.2.1	DHCP Snooping		
3.2.1.1	DHCPv4 & DHCPv6 Snooping Enablement (Manual)	☐	☐
3.2.1.2	DHCPv6 Guard (Manual)	☐	☐
3.3	Multicast		
3.3.1	PIM		
3.3.1.1	PIM Accept-Register (Manual)	☐	☐
3.3.1.2	PIM Accept-RP (Manual)	☐	☐
3.3.1.3	PIM SSM (Manual)	☐	☐
3.3.2	SSDP (Manual)	☐	☐
3.3.3	IGMP Snooping ACL (Manual)	☐	☐
3.3.4	MLD Snooping ACL (Manual)	☐	☐
3.3.5	MSDP Authentication & SA Filtering (Manual)	☐	☐
3.3.6	MSDP SA Cache limit (Manual)	☐	☐
3.3.7	Multicast Boundary ACL (Manual)	☐	☐
3.3.8	Multicast BSR Boundary (Manual)	☐	☐
3.4	IP Source Lockdown (Manual)	☐	☐
3.5	Dynamic ARP Inspection (Manual)	☐	☐
3.6	ND Snooping (Manual)	☐	☐
3.7	RA Guard (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.8	IPv6 Destination Guard (Manual)	☐	☐
4	Control Plane		
4.1	COPP Policing		
4.1.1	Control Plane Policing (Manual)	☐	☐
4.2	Spanning Tree Security		
4.2.1	Spanning Tree BPDU Protect (Manual)	☐	☐
4.2.2	Spanning Tree Root Protect (Manual)	☐	☐
4.3	Control Plane ACL		
4.3.1	Control Plane ACL Management (Manual)	☐	☐

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.3	Hardening Password Rules	☐	☐
1.1.4	Set an Export Password	☐	☐
1.1.5	Enable Enhanced Secure Mode	☐	☐
1.1.6	Default admin account password	☐	☐
1.1.8	Session Management	☐	☐
1.1.10	Using Local RBAC to Limit User Access to Shell	☐	☐
1.2.2	SSH Allow List	☐	☐
1.2.3	SSH Server Port Customization	☐	☐
1.2.4	Recommended Ciphers, MACs, and Algorithms	☐	☐
1.4.1.1	Non Default Community Names, Access Rights & ACL	☐	☐
1.4.3	SNMP Traps	☐	☐
1.5.4.1	Local Accounting	☐	☐
1.5.4.2	Remote Accounting	☐	☐
1.5.5	Per User Management Interface Enablement	☐	☐
1.5.6	Login Privilege Elevation for Administrators	☐	☐
1.7.1	Firmware Validation	☐	☐
1.9.2	https-server idle session management	☐	☐
1.10.1	ServiceOS Password	☐	☐
1.11.2	Configure syslog-client to log using TLS	☐	☐
1.13	Schedule Configuration Backup Job	☐	☐
2.4	IP Directed Broadcast	☐	☐
3.1.1.1	OSPF Passive Interfaces	☐	☐
3.1.2.1	Control Plane ACL for BGP Peering Sessions	☐	☐
3.1.2.3	BGP TTL Security	☐	☐
3.2.1.1	DHCPv4 & DHCPv6 Snooping Enablement	☐	☐
3.2.1.2	DHCPv6 Guard	☐	☐
3.3.1.1	PIM Accept-Register	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.3.1.2	PIM Accept-RP	☐	☐
3.3.1.3	PIM SSM	☐	☐
3.3.2	SSDP	☐	☐
3.3.3	IGMP Snooping ACL	☐	☐
3.3.4	MLD Snooping ACL	☐	☐
3.3.5	MSDP Authentication & SA Filtering	☐	☐
3.3.7	Multicast Boundary ACL	☐	☐
3.3.8	Multicast BSR Boundary	☐	☐
3.5	Dynamic ARP Inspection	☐	☐
3.7	RA Guard	☐	☐
4.3.1	Control Plane ACL Management	☐	☐

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	Create security user group	☐	☐
1.1.2	Securing Password Entry	☐	☐
1.1.3	Hardening Password Rules	☐	☐
1.1.4	Set an Export Password	☐	☐
1.1.5	Enable Enhanced Secure Mode	☐	☐
1.1.6	Default admin account password	☐	☐
1.1.7	RBAC - Customer defined local user groups	☐	☐
1.1.8	Session Management	☐	☐
1.1.9	Verifying Telnet Server is Disabled	☐	☐
1.1.10	Using Local RBAC to Limit User Access to Shell	☐	☐
1.2.1	SSH Public Key Authentication	☐	☐
1.2.2	SSH Allow List	☐	☐
1.2.3	SSH Server Port Customization	☐	☐
1.2.4	Recommended Ciphers, MACs, and Algorithms	☐	☐
1.2.5	Two-factor authentication with the SSH server	☐	☐
1.2.6	SSH Server Key	☐	☐
1.3.1	NTP Authentication	☐	☐
1.3.2	Configuring Time Services	☐	☐
1.4.1.1	Non Default Community Names, Access Rights & ACL	☐	☐
1.4.2.1	SNMP V3	☐	☐
1.4.3	SNMP Traps	☐	☐
1.5.1.1	Radius Server Configuration	☐	☐
1.5.1.2	TACACS Server Configuration	☐	☐
1.5.1.3	RadSec Server Configuration	☐	☐
1.5.2.1	Default & Fallback Local Authentication	☐	☐
1.5.3.1	Local Authorization	☐	☐
1.5.3.2	Remote Authorization	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.5.4.1	Local Accounting	☐	☐
1.5.4.2	Remote Accounting	☐	☐
1.5.5	Per User Management Interface Enablement	☐	☐
1.5.6	Login Privilege Elevation for Administrators	☐	☐
1.6.1	TLS Check Key Usage	☐	☐
1.6.2	TLS Minimum Version	☐	☐
1.7.1	Firmware Validation	☐	☐
1.8.1.1	SFTP and SCP	☐	☐
1.9.1	https-server default enablement	☐	☐
1.9.2	https-server idle session management	☐	☐
1.9.3	Two-factor authentication with the https-server server	☐	☐
1.9.4	Assign a custom certificate to the https-server	☐	☐
1.10.1	ServiceOS Password	☐	☐
1.11.1	Assign a custom certificate to syslog-client	☐	☐
1.11.2	Configure syslog-client to log using TLS	☐	☐
1.13	Schedule Configuration Backup Job	☐	☐
2.1.1	Disable USB and Bluetooth on Device	☐	☐
2.1.3	Disable Unused Physical Interfaces	☐	☐
2.3	Proxy ARP	☐	☐
2.4	IP Directed Broadcast	☐	☐
3.1.1.1	OSPF Passive Interfaces	☐	☐
3.1.1.2	OSPF Neighbor Authentication	☐	☐
3.1.1.3	OSPFv3 Area Authentication and Encryption with IPsec	☐	☐
3.1.2.1	Control Plane ACL for BGP Peering Sessions	☐	☐
3.1.2.2	Authenticate BGP Peers Using MD5	☐	☐
3.1.2.3	BGP TTL Security	☐	☐
3.2.1.1	DHCPv4 & DHCPv6 Snooping Enablement	☐	☐
3.2.1.2	DHCPv6 Guard	☐	☐
3.3.1.1	PIM Accept-Register	☐	☐
3.3.1.2	PIM Accept-RP	☐	☐
3.3.1.3	PIM SSM	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.3.2	SSDP	☐	☐
3.3.3	IGMP Snooping ACL	☐	☐
3.3.4	MLD Snooping ACL	☐	☐
3.3.5	MSDP Authentication & SA Filtering	☐	☐
3.3.6	MSDP SA Cache limit	☐	☐
3.3.7	Multicast Boundary ACL	☐	☐
3.3.8	Multicast BSR Boundary	☐	☐
3.4	IP Source Lockdown	☐	☐
3.5	Dynamic ARP Inspection	☐	☐
3.6	ND Snooping	☐	☐
3.7	RA Guard	☐	☐
3.8	IPv6 Destination Guard	☐	☐
4.2.1	Spanning Tree BPDU Protect	☐	☐
4.3.1	Control Plane ACL Management	☐	☐

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	Create security user group	☐	☐
1.1.2	Securing Password Entry	☐	☐
1.1.3	Hardening Password Rules	☐	☐
1.1.4	Set an Export Password	☐	☐
1.1.5	Enable Enhanced Secure Mode	☐	☐
1.1.6	Default admin account password	☐	☐
1.1.7	RBAC - Customer defined local user groups	☐	☐
1.1.8	Session Management	☐	☐
1.1.9	Verifying Telnet Server is Disabled	☐	☐
1.1.10	Using Local RBAC to Limit User Access to Shell	☐	☐
1.2.1	SSH Public Key Authentication	☐	☐
1.2.2	SSH Allow List	☐	☐
1.2.3	SSH Server Port Customization	☐	☐
1.2.4	Recommended Ciphers, MACs, and Algorithms	☐	☐
1.2.5	Two-factor authentication with the SSH server	☐	☐
1.2.6	SSH Server Key	☐	☐
1.3.1	NTP Authentication	☐	☐
1.3.2	Configuring Time Services	☐	☐
1.4.1.1	Non Default Community Names, Access Rights & ACL	☐	☐
1.4.2.1	SNMP V3	☐	☐
1.4.3	SNMP Traps	☐	☐
1.5.1.1	Radius Server Configuration	☐	☐
1.5.1.2	TACACS Server Configuration	☐	☐
1.5.1.3	RadSec Server Configuration	☐	☐
1.5.2.1	Default & Fallback Local Authentication	☐	☐
1.5.2.2	Limit Login Attempts	☐	☐
1.5.2.3	Remote Authentication - RADIUS/RadSec/TACACS+	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.5.3.1	Local Authorization	☐	☐
1.5.3.2	Remote Authorization	☐	☐
1.5.4.1	Local Accounting	☐	☐
1.5.4.2	Remote Accounting	☐	☐
1.5.5	Per User Management Interface Enablement	☐	☐
1.5.6	Login Privilege Elevation for Administrators	☐	☐
1.6.1	TLS Check Key Usage	☐	☐
1.6.2	TLS Minimum Version	☐	☐
1.7.1	Firmware Validation	☐	☐
1.8.1.1	SFTP and SCP	☐	☐
1.9.1	https-server default enablement	☐	☐
1.9.2	https-server idle session management	☐	☐
1.9.3	Two-factor authentication with the https-server server	☐	☐
1.9.4	Assign a custom certificate to the https-server	☐	☐
1.10.1	ServiceOS Password	☐	☐
1.11.1	Assign a custom certificate to syslog-client	☐	☐
1.11.2	Configure syslog-client to log using TLS	☐	☐
1.13	Schedule Configuration Backup Job	☐	☐
2.1.1	Disable USB and Bluetooth on Device	☐	☐
2.1.3	Disable Unused Physical Interfaces	☐	☐
2.3	Proxy ARP	☐	☐
2.4	IP Directed Broadcast	☐	☐
3.1.1.1	OSPF Passive Interfaces	☐	☐
3.1.1.2	OSPF Neighbor Authentication	☐	☐
3.1.1.3	OSPFv3 Area Authentication and Encryption with IPsec	☐	☐
3.1.2.1	Control Plane ACL for BGP Peering Sessions	☐	☐
3.1.2.2	Authenticate BGP Peers Using MD5	☐	☐
3.1.2.3	BGP TTL Security	☐	☐
3.2.1.1	DHCPv4 & DHCPv6 Snooping Enablement	☐	☐
3.2.1.2	DHCPv6 Guard	☐	☐
3.3.1.1	PIM Accept-Register	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.3.1.2	PIM Accept-RP	☐	☐
3.3.1.3	PIM SSM	☐	☐
3.3.2	SSDP	☐	☐
3.3.3	IGMP Snooping ACL	☐	☐
3.3.4	MLD Snooping ACL	☐	☐
3.3.5	MSDP Authentication & SA Filtering	☐	☐
3.3.6	MSDP SA Cache limit	☐	☐
3.3.7	Multicast Boundary ACL	☐	☐
3.3.8	Multicast BSR Boundary	☐	☐
3.4	IP Source Lockdown	☐	☐
3.5	Dynamic ARP Inspection	☐	☐
3.6	ND Snooping	☐	☐
3.7	RA Guard	☐	☐
3.8	IPv6 Destination Guard	☐	☐
4.1.1	Control Plane Policing	☐	☐
4.2.1	Spanning Tree BPDU Protect	☐	☐
4.3.1	Control Plane ACL Management	☐	☐

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.14	Create Hostname	☐	☐

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	Create security user group	☐	☐
1.1.3	Hardening Password Rules	☐	☐
1.1.4	Set an Export Password	☐	☐
1.1.5	Enable Enhanced Secure Mode	☐	☐
1.1.6	Default admin account password	☐	☐
1.1.7	RBAC - Customer defined local user groups	☐	☐
1.1.8	Session Management	☐	☐
1.1.9	Verifying Telnet Server is Disabled	☐	☐
1.1.10	Using Local RBAC to Limit User Access to Shell	☐	☐
1.2.2	SSH Allow List	☐	☐
1.2.3	SSH Server Port Customization	☐	☐
1.2.4	Recommended Ciphers, MACs, and Algorithms	☐	☐
1.2.5	Two-factor authentication with the SSH server	☐	☐
1.4.1.1	Non Default Community Names, Access Rights & ACL	☐	☐
1.4.3	SNMP Traps	☐	☐
1.5.2.1	Default & Fallback Local Authentication	☐	☐
1.5.4.1	Local Accounting	☐	☐
1.5.4.2	Remote Accounting	☐	☐
1.5.5	Per User Management Interface Enablement	☐	☐
1.5.6	Login Privilege Elevation for Administrators	☐	☐
1.7.1	Firmware Validation	☐	☐
1.8.1.1	SFTP and SCP	☐	☐
1.9.1	https-server default enablement	☐	☐
1.9.2	https-server idle session management	☐	☐
1.10.1	ServiceOS Password	☐	☐
1.11.2	Configure syslog-client to log using TLS	☐	☐
1.13	Schedule Configuration Backup Job	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.3	Proxy ARP	☐	☐
2.4	IP Directed Broadcast	☐	☐
3.1.1.1	OSPF Passive Interfaces	☐	☐
3.1.2.1	Control Plane ACL for BGP Peering Sessions	☐	☐
3.1.2.3	BGP TTL Security	☐	☐
3.2.1.1	DHCPv4 & DHCPv6 Snooping Enablement	☐	☐
3.2.1.2	DHCPv6 Guard	☐	☐
3.3.1.1	PIM Accept-Register	☐	☐
3.3.1.2	PIM Accept-RP	☐	☐
3.3.1.3	PIM SSM	☐	☐
3.3.2	SSDP	☐	☐
3.3.3	IGMP Snooping ACL	☐	☐
3.3.4	MLD Snooping ACL	☐	☐
3.3.5	MSDP Authentication & SA Filtering	☐	☐
3.3.7	Multicast Boundary ACL	☐	☐
3.3.8	Multicast BSR Boundary	☐	☐
3.5	Dynamic ARP Inspection	☐	☐
3.7	RA Guard	☐	☐
4.3.1	Control Plane ACL Management	☐	☐

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	Create security user group	☐	☐
1.1.2	Securing Password Entry	☐	☐
1.1.3	Hardening Password Rules	☐	☐
1.1.4	Set an Export Password	☐	☐
1.1.5	Enable Enhanced Secure Mode	☐	☐
1.1.6	Default admin account password	☐	☐
1.1.7	RBAC - Customer defined local user groups	☐	☐
1.1.8	Session Management	☐	☐
1.1.9	Verifying Telnet Server is Disabled	☐	☐
1.1.10	Using Local RBAC to Limit User Access to Shell	☐	☐
1.2.1	SSH Public Key Authentication	☐	☐
1.2.2	SSH Allow List	☐	☐
1.2.3	SSH Server Port Customization	☐	☐
1.2.4	Recommended Ciphers, MACs, and Algorithms	☐	☐
1.2.5	Two-factor authentication with the SSH server	☐	☐
1.2.6	SSH Server Key	☐	☐
1.3.1	NTP Authentication	☐	☐
1.3.2	Configuring Time Services	☐	☐
1.4.1.1	Non Default Community Names, Access Rights & ACL	☐	☐
1.4.2.1	SNMP V3	☐	☐
1.4.3	SNMP Traps	☐	☐
1.5.1.1	Radius Server Configuration	☐	☐
1.5.1.2	TACACS Server Configuration	☐	☐
1.5.1.3	RadSec Server Configuration	☐	☐
1.5.2.1	Default & Fallback Local Authentication	☐	☐
1.5.2.3	Remote Authentication - RADIUS/RadSec/TACACS+	☐	☐
1.5.3.1	Local Authorization	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.5.3.2	Remote Authorization	☐	☐
1.5.4.1	Local Accounting	☐	☐
1.5.4.2	Remote Accounting	☐	☐
1.5.5	Per User Management Interface Enablement	☐	☐
1.5.6	Login Privilege Elevation for Administrators	☐	☐
1.6.1	TLS Check Key Usage	☐	☐
1.6.2	TLS Minimum Version	☐	☐
1.7.1	Firmware Validation	☐	☐
1.8.1.1	SFTP and SCP	☐	☐
1.9.1	https-server default enablement	☐	☐
1.9.2	https-server idle session management	☐	☐
1.9.3	Two-factor authentication with the https-server server	☐	☐
1.9.4	Assign a custom certificate to the https-server	☐	☐
1.10.1	ServiceOS Password	☐	☐
1.11.1	Assign a custom certificate to syslog-client	☐	☐
1.11.2	Configure syslog-client to log using TLS	☐	☐
1.13	Schedule Configuration Backup Job	☐	☐
2.1.1	Disable USB and Bluetooth on Device	☐	☐
2.1.3	Disable Unused Physical Interfaces	☐	☐
2.3	Proxy ARP	☐	☐
2.4	IP Directed Broadcast	☐	☐
3.1.1.1	OSPF Passive Interfaces	☐	☐
3.1.1.2	OSPF Neighbor Authentication	☐	☐
3.1.1.3	OSPFv3 Area Authentication and Encryption with IPsec	☐	☐
3.1.2.1	Control Plane ACL for BGP Peering Sessions	☐	☐
3.1.2.2	Authenticate BGP Peers Using MD5	☐	☐
3.1.2.3	BGP TTL Security	☐	☐
3.2.1.1	DHCPv4 & DHCPv6 Snooping Enablement	☐	☐
3.2.1.2	DHCPv6 Guard	☐	☐
3.3.1.1	PIM Accept-Register	☐	☐
3.3.1.2	PIM Accept-RP	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.3.1.3	PIM SSM	☐	☐
3.3.2	SSDP	☐	☐
3.3.3	IGMP Snooping ACL	☐	☐
3.3.4	MLD Snooping ACL	☐	☐
3.3.5	MSDP Authentication & SA Filtering	☐	☐
3.3.6	MSDP SA Cache limit	☐	☐
3.3.7	Multicast Boundary ACL	☐	☐
3.3.8	Multicast BSR Boundary	☐	☐
3.4	IP Source Lockdown	☐	☐
3.5	Dynamic ARP Inspection	☐	☐
3.6	ND Snooping	☐	☐
3.7	RA Guard	☐	☐
3.8	IPv6 Destination Guard	☐	☐
4.2.1	Spanning Tree BPDU Protect	☐	☐
4.3.1	Control Plane ACL Management	☐	☐

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	Create security user group	☐	☐
1.1.2	Securing Password Entry	☐	☐
1.1.3	Hardening Password Rules	☐	☐
1.1.4	Set an Export Password	☐	☐
1.1.5	Enable Enhanced Secure Mode	☐	☐
1.1.6	Default admin account password	☐	☐
1.1.7	RBAC - Customer defined local user groups	☐	☐
1.1.8	Session Management	☐	☐
1.1.9	Verifying Telnet Server is Disabled	☐	☐
1.1.10	Using Local RBAC to Limit User Access to Shell	☐	☐
1.2.1	SSH Public Key Authentication	☐	☐
1.2.2	SSH Allow List	☐	☐
1.2.3	SSH Server Port Customization	☐	☐
1.2.4	Recommended Ciphers, MACs, and Algorithms	☐	☐
1.2.5	Two-factor authentication with the SSH server	☐	☐
1.2.6	SSH Server Key	☐	☐
1.3.1	NTP Authentication	☐	☐
1.3.2	Configuring Time Services	☐	☐
1.4.1.1	Non Default Community Names, Access Rights & ACL	☐	☐
1.4.2.1	SNMP V3	☐	☐
1.4.3	SNMP Traps	☐	☐
1.5.1.1	Radius Server Configuration	☐	☐
1.5.1.2	TACACS Server Configuration	☐	☐
1.5.1.3	RadSec Server Configuration	☐	☐
1.5.2.1	Default & Fallback Local Authentication	☐	☐
1.5.2.3	Remote Authentication - RADIUS/RadSec/TACACS+	☐	☐
1.5.3.1	Local Authorization	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.5.3.2	Remote Authorization	☐	☐
1.5.4.1	Local Accounting	☐	☐
1.5.4.2	Remote Accounting	☐	☐
1.5.5	Per User Management Interface Enablement	☐	☐
1.5.6	Login Privilege Elevation for Administrators	☐	☐
1.6.1	TLS Check Key Usage	☐	☐
1.6.2	TLS Minimum Version	☐	☐
1.7.1	Firmware Validation	☐	☐
1.8.1.1	SFTP and SCP	☐	☐
1.9.1	https-server default enablement	☐	☐
1.9.2	https-server idle session management	☐	☐
1.9.3	Two-factor authentication with the https-server server	☐	☐
1.9.4	Assign a custom certificate to the https-server	☐	☐
1.10.1	ServiceOS Password	☐	☐
1.11.1	Assign a custom certificate to syslog-client	☐	☐
1.11.2	Configure syslog-client to log using TLS	☐	☐
1.13	Schedule Configuration Backup Job	☐	☐
2.1.1	Disable USB and Bluetooth on Device	☐	☐
2.1.3	Disable Unused Physical Interfaces	☐	☐
2.3	Proxy ARP	☐	☐
2.4	IP Directed Broadcast	☐	☐
3.1.1.1	OSPF Passive Interfaces	☐	☐
3.1.1.2	OSPF Neighbor Authentication	☐	☐
3.1.1.3	OSPFv3 Area Authentication and Encryption with IPsec	☐	☐
3.1.2.1	Control Plane ACL for BGP Peering Sessions	☐	☐
3.1.2.2	Authenticate BGP Peers Using MD5	☐	☐
3.1.2.3	BGP TTL Security	☐	☐
3.2.1.1	DHCPv4 & DHCPv6 Snooping Enablement	☐	☐
3.2.1.2	DHCPv6 Guard	☐	☐
3.3.1.1	PIM Accept-Register	☐	☐
3.3.1.2	PIM Accept-RP	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.3.1.3	PIM SSM	☐	☐
3.3.2	SSDP	☐	☐
3.3.3	IGMP Snooping ACL	☐	☐
3.3.4	MLD Snooping ACL	☐	☐
3.3.5	MSDP Authentication & SA Filtering	☐	☐
3.3.6	MSDP SA Cache limit	☐	☐
3.3.7	Multicast Boundary ACL	☐	☐
3.3.8	Multicast BSR Boundary	☐	☐
3.4	IP Source Lockdown	☐	☐
3.5	Dynamic ARP Inspection	☐	☐
3.6	ND Snooping	☐	☐
3.7	RA Guard	☐	☐
3.8	IPv6 Destination Guard	☐	☐
4.1.1	Control Plane Policing	☐	☐
4.2.1	Spanning Tree BPDU Protect	☐	☐
4.3.1	Control Plane ACL Management	☐	☐

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.14	Create Hostname	☐	☐

Appendix: Change History

Date	Version	Changes for this version